情報システム調達のための技術参照モデル（TRM）

平成 22 年度版

2011 年　6 月

経済産業省　商務情報政策局　情報処理振興課

独立行政法人　情報処理推進機構

目次

1. 序文 4
1.1. 背景 4
1.2. 目的 4
1.3. 読者 5
1.4. 適用範囲 5
1.5. 文書の構成 5
1.6. 平成 21 年度版からの改訂の概要 6
1.7. 平成 23 年度版の改訂の予定 6
2. 概要 7
2.1. 技術参照モデルの位置づけ 7
2.2. 本技術参照モデルの構成 9
3. 定義(技術の分類) 15
4. 調達パターンとモデル及び情報システム設計の指針 21
4.1. 機能構成モデル 21
4.2. 物理構成モデル 29
4.3. 役務の分類 31
4.4. 業務アプリケーションの考え方 34
4.5. 共通データベースの考え方 39
4.6. 府省共通システム導入の考え方 41
4.7. 仮想化技術 42
4.8. クラウド利用者の立場からの考え方 45
4.9. クラウドを構築する立場からの考え方 55
4.10. セキュリティの考え方 59
4.11. グリーン IT 導入の考え方 68
4.12. IPv6 対応上の留意点 70
5. 技術ドメイン解説 71
5.1. BI/DWH/ETL 72
5.2. EAI 83
5.3. iDC・設備 85
5.4. SOA 関連機能 89
5.5. 保守環境 96
5.6. サーバ 105
5.7. ストレージ 116
5.8. 共通 PC・オフィスプリンタ 120
5.9. 運用管理 / セキュリティ 137
5.10. EIP 167
5.11. 公開 Web サーバ 170
5.12. グループウェア, ファイルサーバ, メールサーバ 178

5.13. 統合アカウント管理・認証・認可(アクセス制御)....188
5.14. 統合ディレクトリ....195
5.15. WAN, 省内 LAN, DNS/DHCP/Proxy, リモートアクセス....199
5.16. ワークフロー、BAM....221
5.17. ドメイン共通....222
6. 役務調達....223
6.1. 全体計画策定支援....225
6.2. 調達支援....232
6.3. システム構築(設計・開発)....251
6.4. 運用....277
6.5. ヘルプデスク....302
6.6. 保守....326
6.7. 機器調達付帯作業....379
6.8. iDC 設備調達付帯作業....398
6.9. ネットワーク調達....420
6.10. クラウドサービス....458
6.11. クラウド構築....459
6.12. セキュリティ....460
6.13. その他....490
7. 推奨される技術標準....491
7.1. 「情報システムに係る相互運用性フレームワーク」による技術標準要件....491
7.2. 「TRM 第 1 版:妥当性検証報告書」における技術標準の評価項目....493
7.3. 推奨される技術標準の選定指針....494
7.4. 推奨される技術標準....499
付録1 調達事例....504
付録2 役務調達仕様書例....508
付録3 別表 暗号アルゴリズムの移行指針について....514
付録4 参考文献....516

1.序文

本書は、情報システムに係る政府調達に関するものであり、「情報システムに係る政府調達の基本指針」を補完する参考資料である。

1.1.背景

2007年7月より施行された「情報システムに係る政府調達の基本指針」(2007年(平成19年)3月1日 各府省情報統括責任者(CIO)連絡会議決定 以下 調達指針)に従い、分離調達によって情報システムを構築する場合、分離調達された個々のシステムを構築するベンダーごとに利用する技術、特に個々のシステムが提供するサービス呼び出しのためのインタフェースが異なると、個別業務システムと共通基盤システム間の相互運用性が失われ、結果として分離調達された個々のシステムの統合が困難になることがある。また、各府省ではホームページや電子申請システムなどの国民との窓口となるシステムを構築しているが、利用者(国民)が使用するクライアントシステムに必要となるソフトウェアが府省ごとに異なったり、特定の Web ブラウザが必要であったり、OS や Java 等の実行環境のバージョンが異なるため、利用する府省ごとにクライアントシステムを用意しなければならないなど、必ずしも利用者側の立場に立ったものとなっていないことがある。さらに、府省ごとに調達・構築する情報システムが、調達指針、「業務・システム最適化指針(ガイドライン)」(2006 年(平成18年)3月 31 日各府省情報統括責任者(CIO)連絡会議決定 以下 最適化指針)及び「情報システムに係る相互運用性フレームワーク」(2007年(平成19年) 6月 29 日 経済産業省発表 以下 相互運用性フレームワーク)に従った最適なものであったとしても、他システムへの流用が困難であるなど、政府全体として必ずしも最適なものとなっていないことがある。

1.2.目的

本「情報システム調達のための技術参照モデル(TRM)」(以下 技術参照モデル)は、

- 利用者の利便性の向上
- 分離調達における確実なシステム構築
- 業務・システムのライフサイクルを通したトータルコストの最適化
- 調達効率の向上

を目指し、最適な情報システムの調達及び構築に資する以下の技術情報を提供する。

- 調達指針に従った分離調達及び統合を容易にするための技術指針 (第 4 章)
- 仮想化、セキュリティ、クラウド、グリーン IT に関する技術指針(第4章)
- 典型的な調達パターンを意識した機能構成モデル (第 4 章)
- 典型的な政府情報システムを意識した物理構成モデル (第 4 章)
- 物品調達における分離調達の最小単位となりうる技術ドメインの解説 (第 5 章)

- 物品調達における技術ドメインごとの中立的な要件の記述例（第 5 章）
- 役務調達における調達分類ごとの要件記述のポイント（第6章）
- 相互運用性があり、最適なシステム構築のために優先的に採用すべきオープンな標準（第7章）
- 本書の内容を補完するために参照できる事例集（調達事例）
- セキュリティに関する注意事項(暗号移行問題)

1.3.読者

本技術参照モデルは、主たる読者として以下の人々を想定している。ただし、政府情報システム以外への適用に関しては、それぞれの調達・システム構築ポリシーに合わせて、調達単位の粒度及び優先的に採用する技術・オープンな標準に関してカスタマイズが必要になる可能性がある。

- 各府省、独立行政法人及び地方自治体の CIO,CIO 補佐官及び支援スタッフ
- 各府省、独立行政法人及び地方自治体の情報システム設計・計画・運用担当官
- 各府省、独立行政法人及び地方自治体の調達担当官
- 調達支援事業者
- 情報システムに関する政府調達の応札者

1.4.適用範囲

本技術参照モデルが提供する技術情報の主たる適用範囲は、

- 中央省庁の政府情報システム
- 独立行政法人の情報システム
- 地方自治体の情報システム

であるが、その他民間の情報システムの調達・構築にも参考となるように書かれている。ただし、中央省庁の情報システム以外への適用に関しては、それぞれの調達・システム構築のポリシーに合わせてカスタマイズを行う必要がある。

本技術参照モデルは情報システムに係る政府調達における現場の要請、要求事項及び要件の変化を反映して定期的に改訂される。

本技術参照モデルは、調達指針で示されている、曖昧な要求要件の排除、現実的な要求要件の記載、特定のハードウェア及びソフトウェアについて有利な要求要件とならないような中立的な要求要件の記載に資するように作成されている。

1.5.文書の構成

情報システム調達のための技術参照モデル関連文書の構成は、技術情報を記載した本技術参照モデルと、本技術参照モデルの活用の仕方を解説した「情報システム調達のための技術参照モデル(TRM)活用の

手引き」(以下　活用の手引き)並びに別冊付録として Web 上で公開される技術一覧表及び技術解説からなる。

1.6.平成 21 年度版からの改訂の概要

平成 22 年度版では、平成 21 年度版に対し、以下に挙げる内容の拡充及び見直しを行った。

- 役務調達の分類の追加
- 役務調達における調達分類ごとにおける要件記述のポイントの追加
- 仮想化に関する技術指針の追加
- クラウド活用に関する技術指針の追加
- クラウド構築に関する技術指針の追加
- 情報セキュリティの拡充
- 推奨される技術標準の選定指針を詳細に記載
- 技術一覧表及び技術解説を技術参照モデルから分離し、Web 上で公開

1.7.平成 23 年度版の改訂の予定

平成 23 年度版では、以下に挙げる内容の拡充を計画している。

- 物品調達における技術要件の見直し
- 役務調達における典型的な要件記述
- クラウド利用に関する典型的な要件記述
- クラウド構築に関する典型的な要件記述
- 調達仕様書におけるオープンな標準の活用

2.概要

本章では、本技術参照モデルの概要を説明する。

2.1.技術参照モデルの位置づけ

本技術参照モデルは、最適化指針が示す政府情報システムの最適化に関する指針、調達指針が示す政府調達に関する指針、相互運用性フレームワークが示す情報システム間の相互運用性に関する指針、政府機関統一基準が示す情報システムに係るセキュリティの指針を、資料提供招請(RFI)、提案依頼(RFP)及び調達仕様書レベルに落とし込むのに資する技術情報を示している。

2.1.1.最適化指針との関係

本技術参照モデルは、最適化指針に記載された下記の指針の推進に資する技術情報を示している。

【指針 4-1】

複数の府省、部局、課室等で同様の処理が行われている業務について、当該業務の全部又は一部について情報システムを活用し、同一の業務処理方法を適用する場合は、情報システムの一元化・集中化を図り、汎用的な一の情報システムを関係する複数の府省、部局、課室等で共同利用する。

各府省でデータの分散管理を行うことが適切な場合においても、アプリケーション機能の一元化・集中化を図るとともに、データ管理機能の仕様を統一することにより、相互互換性を確保しつつ、システム開発・運用の費用低減を図る。

【指針 4-2】

各府省内の LAN は、一府省あたり一システムとし、メールシステムその他の基本システムの統一化及び運用管理業務の集中化を図る。

【指針 4-3】

情報システムを利用する職員のコンピュータ端末は、各府省内で整備される LAN の利用端末を用いるものとし、また、情報システムのサーバ機能及びこれを利用する職員のコンピュータ端末の間を結ぶネットワーク回線は、府省内で整備される LAN その他の基盤となるネットワークを活用するものとする。

【指針 4-4】

府省間を結ぶネットワーク回線及び国の行政機関と地方公共団体を結ぶネットワーク回線は、それぞれ霞が関 WAN 及び総合行政ネットワーク(LGWAN)を活用するものとする。

【指針 4-5】

情報システムを構成するハードウェア及びソフトウェア並びに通信プロトコルは、国際標準又は事実上の

標準を採用し、オープンシステムとする。

【指針 4-6】

ホームページ等のインターネットで提供する情報システムは、インターネット接続口の集約を図り、関係する複数の情報システムに係る情報セキュリティ対策を包括的に行う。

【指針 4-7】

複数の府省で共同利用する情報システム並びに国民生活及び社会経済活動に密接に関連する情報システムのうち、情報システムの完全性及び可用性が高度に求められるものについては、バックアップ・システムを整備する。

2.1.2.調達指針との関係

本技術参照モデルは、調達指針と整合し、調達指針に従った政府調達を容易にし、システム構築を円滑に行うための技術情報を示している。

- 設計・開発の工程における分離調達
- 設計・開発等の工程の管理
- 提案に不可欠な情報の網羅
- ハードウェアとソフトウェアの分離調達
- 設計・開発から移行までの工程、運用の工程及び保守の工程の分離調達
- 曖昧な要求要件の排除
- オープンな標準に基づく要求要件の記載

注 1) 「オープンな標準」とは、原則として、①開かれた参画プロセスの下で合意され、具体的仕様が実装可能なレベルで公開されていること、②誰もが採用可能であること、③技術標準が実現された製品が市場に複数あること、のすべてを満たしている技術標準をいう。

注2) 調達指針及び「情報システムに係る政府調達の基本指針」実務手引書(第2版)(総務省行政管理局 2007年7月1日発表 以下、実務手引書)における「共通基盤システム」と「H/W 基盤」を合わせた総称名として、本技術参照モデルでは「共通基盤」と呼称している。事業者についても同様に、「共通基盤システム事業者」と「H/W 基盤事業者」を合わせた総称名として、本技術参照モデルでは「共通基盤事業者」と呼称している。

2.1.3.相互運用性フレームワークとの関係

本技術参照モデルは、相互運用性フレームワークと整合し、相互運用性フレームワークが提示する情報システムに係る政府方針及び相互運用性に関する指針に従った調達仕様書の作成に資する技術情報を示している。

- 要求仕様の中立性に関する方針
- オープンな標準の優先に関する方針
- 最適な情報システムの選定に関する方針
- オープン化の方針

また、本技術参照モデルは、相互運用性フレームワークが提示する下記の指針に従い、疎結合でサービスを結合することによって個別業務システムと共通基盤システムを結合することを推奨している。

指針: 分離調達を行う際に、応札者を増やすためには、分離される機能単位が稼動する物理的なコンピュータや、プラットフォームに対しての制限を与えないことが望ましい。そのためには、サービス呼び出しのインタフェースはプラットフォーム非依存となる必要があり、それぞれのサービスは非同期かつ疎結合で結合される必要がある。

2.1.4.政府機関統一基準との関係

本技術参照モデルは、政府機関統一基準と整合し、政府機関統一基準が提示する情報システムに係るセキュリティの政府指針に従った調達仕様書の作成に資する技術情報を示している。

注:政府機関統一基準は、2011 年 4 月 23 日に最新版が公表された。

http://www.nisc.go.jp/active/general/kijun01.html

2.1.5. セキュリティ・バイ・デザイン及びリスク要件リファレンスモデルとの関係

本技術参照モデルは、その 4.10 節でセキュリティ・バイ・デザインとリスク要件リファレンスモデルの概要の紹介を行い、セキュリティに関する考え方の指針を提供している。

2.1.6. 政府共通プラットフォームとの関係

本技術参照モデルは、その 4.8 節でクラウドを利用するための考え方を示しているが、その考え方は政府共通プラットフォームを利用する際にも活用できる。

2.2.本技術参照モデルの構成

3 章以降、本技術参照モデルは、次に挙げる技術情報を示す。

2.2.1.第 3 章 定義(技術の分類)

第 3 章では、本技術参照モデル及び別冊の技術一覧表で取り扱う技術の分類を示す。

本技術参照モデルでは、調達者と応札者があいまい性の少ない技術的な会話を行えるようにするために、調達者と応札者の両方の視点から対象技術を分類することにした。第 3 章では応札者の視点から技術の分類を行っており、IT システムの構造を階層化し、TRM のフレームワークとして体系化した上で、技術要素をその利用目的や特性によって分類している。

技術一覧表分類			
大分類	中分類	技術 技術ドメイン解説上の相当機能	技術細目
ハードウェアプラットフォーム	PC・オフィスプリンタ	パーソナルコンピュータ	
		シンクライアント	
		オフィス・プリンタ装置	
	サーバ	サーバハードウェア	サーバハードウェア
	ストレージ	ディスクストレージ	
		テープストレージ	
	ネットワーク	LAN	スイッチ
			セキュア無線 LAN
		WAN	ルータ
		リモートアクセス	
		回線サービス	
オペレーティングプラットフォーム	PC・オフィスプリンタ	共通オペレーション環境	OS カーネル
			周辺機器サポート
			コマンドライン環境
			Web ブラウザ
			動画閲覧
	サーバ	サーバ・オペレーティング・システム	OS サービス
		シンクライアントサーバ	
	ネットワーク	DNS/DHCP/Proxy	DNS サーバ
			DHCP サーバ
			Proxy サーバ
		VoIP	
アプリケーションプラットフォーム	アプリケーション実行環境	Web サーバ	
		AP サーバ	
	データ管理	メタデータレジストリ	
		DB サーバ	
		ファイル共有	
		統合ディレクトリ	
	データ交換/連携	EAI	
		アダプタ	
		レガシー連携	

表 2.2-1 技術一覧表抜粋

調達者の視点から同時に調達を行う単位として分割した技術ドメインを、TRM のフレームワーク上の階層図上にマップすると、それぞれの技術ドメインは下図のような階層に位置する。

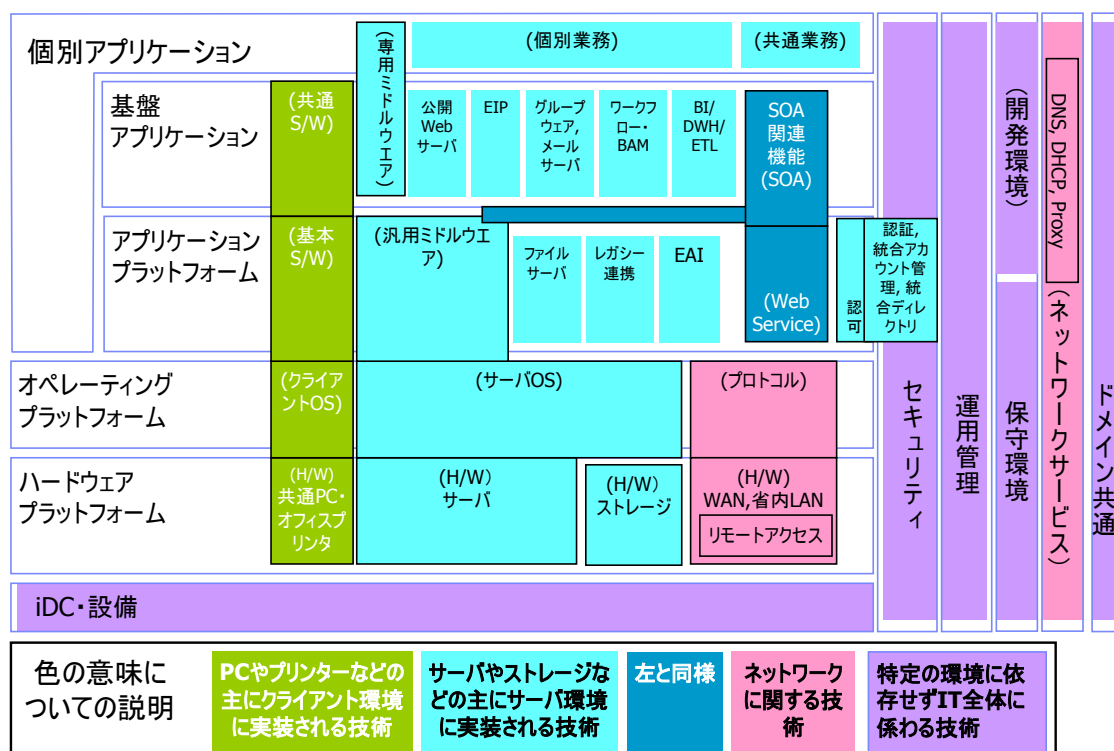



図 2.2-2 TRM のフレームワークと技術ドメインのマップ

2.2.2.第 4 章　調達パターンとモデル及び情報システム設計の指針

第 4 章では、物品調達を調達者の視点から調達対象となる機能を調達単位ごとにパターン化して、同時に調達することが多いと考えられる技術ドメインに分割し、その技術ドメインごとに調達すべき役務と物品を示している。また機能構成モデルの各ドメインが、各府省の情報システムの物理構成上どこに位置すべきものであるかを示している。ただし、構成図上の各要素のすべてを必ずしも物理的に別々のハードウェア上に実現する必要はないことに注意する必要がある。最適化の観点から、各技術ドメインで提供する機能はサーバ統合により一つのサーバハードウェア上で実現される場合もあれば、以前の調達で調達されたハードウェアもしくは回線装置が活用できる場合もある。実際の調達に際しては、必ず最適化を行い、不必要な物品もしくは役務の調達を行わないよう、注意を払う必要がある。

また第 4 章では、最適化指針、調達指針、相互運用性フレームワークを補完する目的で、調達を行う情報システムの設計、資料提供招請(RFI)、提案依頼(RFP)、調達仕様書の作成の際に従うべき指針として、業務アプリケーションの考え方、共通データベースの考え方、府省共通システム導入の考え方、グリーン IT 導入の考え方、セキュリティの考え方、仮想化の考え方、クラウドを利用する立場からの考え方、クラウドを構築する立場からの考え方を示している。

2.2.3.第 5 章　技術ドメイン解説

第 5 章では、物品調達について調達者の視点から各技術ドメインを解説し、調達仕様書に記述すべき要件のうち汎用的な要件を要件の記述例として示している。ここに挙げた機能要件、非機能要件の例は、本技術参照モデル発行時においてその要件を満たす技術又は製品が存在し、かつ日本国内での実績を考慮し、現実的な要件となっているが、あくまで汎用的な調達を意識して書かれたものであるので、実際の調達に際

しては調達対象の個別事情を考慮して、{ }で示されたパラメタ(可変数値)の調整、【 】で示された例示の調整及び選択、必要な要件の追加、不要な要件の削除等のカスタマイズを行う必要がある。ただし、これらのカスタマイズでは不必要に高い制限値、必須ではない要件の追加を行わないように十分検討を行う必要がある。また結果として特定の技術や製品を指定してしまわないように注意しなければならない。

また、必ずしも技術ドメインを構成する要素のすべてを調達する必要がない旨注意する必要がある。技術ドメインを構成する要素のうち幾つかは以前の調達で調達したものが利用可能かもしれないし、同時に調達を行う他の技術ドメインのものが利用可能かもしれない。第5章の記述内容を実際の調達仕様書に活用する際には、最適化を行い、既存の資産の活用及びほかの技術ドメインの調達との重複を避けることが望ましい。

2.2.4. 第6章 役務調達

第6章では、役務調達について調達者の視点から調達対象の役務を分類し、その調達分類ごとに仕様書に記載すべき役務の概要を示す。その詳細として事前に調達者側が用意すべき情報、役務調達で作成される成果物、仕様書に記載すべきポイント及び説明、案件・情報システムの特性等による留意点、セキュリティに関する留意点等の情報を提供している。これらの記述は第 5 章のそれとは異なり、仕様書に転記することを意図して書かれてはいない。役務調達は物品調達に比べて個別の要素が大きいので、前工程となる役務調達の成果を十分に活用して仕様書を作成する必要がある。

図 2.2-3 役務調達の分類

表 2. 2－4　各役務に関する説明

役務	対象とする役務作業
6.1　全体計画策定支援	システム化構想の立案、システム化計画の立案
6.2　調達支援	要件定義の実施、調達方針・調達方式決定、調達仕様書の作成、意見招請、受注者の評価、プロジェクト管理などの府省の調達業務を支援する役務作業
6.3　システム構築(設計・開発)	情報システムの設計、開発、移行、運用・保守設計などの情報システムの構築にかかわる役務作業
6.4　運用	情報システムの運用業務にかかわる役務作業 (6.5　ヘルプデスクは 6.4 の作業の一部に位置づけられるが、本章では分けて記載を行っている)
6.5　ヘルプデスク	システム運用業務における利用者からの問い合わせに対応するヘルプデスク業務にかかわる役務作業
6.6　保守	情報システムの障害の訂正、納入後のシステム・ソフトウェア製品の修正、変更された環境への適合など、情報システムの保守を行う役務作業
6.7　機器調達付帯作業	情報システムに必要な機器(ハードウェアと不可分な OS 等の既製のソフトウェアを含む)の設置・設定等、機器調達に付帯して発生する役務作業　(※保守は含まない)
6.8　iDC 設備調達付帯作業	受注者が用意する施設(データセンター)への各種機器の設置、設定、対象システムの運用監視(及びそれに付帯する業務)、などの役務作業
6.9　ネットワーク調達	LAN、WAN 等の構内ネットワークの構築にかかわる役務、WAN 等の広域ネットワークサービスやインターネットサービス等のサービスの調達に付随する役務作業
6.10　クラウドサービス	クラウドシステムのサービスを利用する役務作業
6.11　クラウド構築	クラウドシステムを構築する役務作業
6.12　セキュリティ	本節では各役務の調達におけるセキュリティの留意点、情報システムの構築時におけるセキュリティの検討方法を記載
6.13　その他(作成予定)	業務パッケージソフトウェアの調達など、6.1～6.12 に分類されない役務作業

2.2.5. 第 7 章　推奨される技術標準

第7章では、特に政府情報システムの調達の際に優先的に調達すべきオープンな標準を示している。これらのオープンな標準は、調達指針が示す分離調達を実施する観点で選ばれたものであり、調達される技術すべてを網羅するものではない。また、オープンな標準といえども相互運用性を必要としないレベルまで標準を指定することは、それに適合する製品・技術の選択肢を狭めることもあるので、調達仕様書の作成にあたっては参照するオープンな標準は、分離調達を行う情報システムの要素間のインタフェース、既存の環境と新規調達を行う情報システムの要素間のインタフェースにとどめ、より細かいレベルでのオープンな標準の活用は応札者の提案にゆだねることが望ましい。

2.2.6.付録1　調達事例

付録1では、本技術参照モデルの記述を補完し、品質の高い調達仕様書の作成を容易にする目的で、実際行われた政府調達の調達仕様書の例を掲載している。実際の調達仕様書の作成に際しては、本文の記述とともに、これらの事例を参照することが望ましい。また、本技術参照モデルに掲載されていない事例は、総務省及び各府省の Web ページ上で参照することが可能である。

2.2.7.付録2　役務調達仕様書の例

付録2では、本技術参照モデルの第6章各節の記述のもととなった実際の役務調達仕様書の一覧を示している。

2.2.8. 付録3　別表暗号移行問題

付録3では、現在広く使用されている暗号アルゴリズム SHA-1 及び RSA1024 の安全な暗号方式への移行の必要性を説明している。

2.2.9. 付録4　参考文献

付録4では、本技術参照モデルを理解する上で参考となる文書を上げ、その入手法を示している。

3.定義(技術の分類)

本技術参照モデルでは、調達者と応札者があいまい性の少ない技術的な会話を行えるようにするために、調達者と応札者の両方の視点から対象技術を分類することにした。第 3 章では応札者の視点から技術の分類を行っており、IT システムの構造を層化し、TRM のフレームワークとして体系化した上で、技術要素をその利用目的や特性によって分類している。

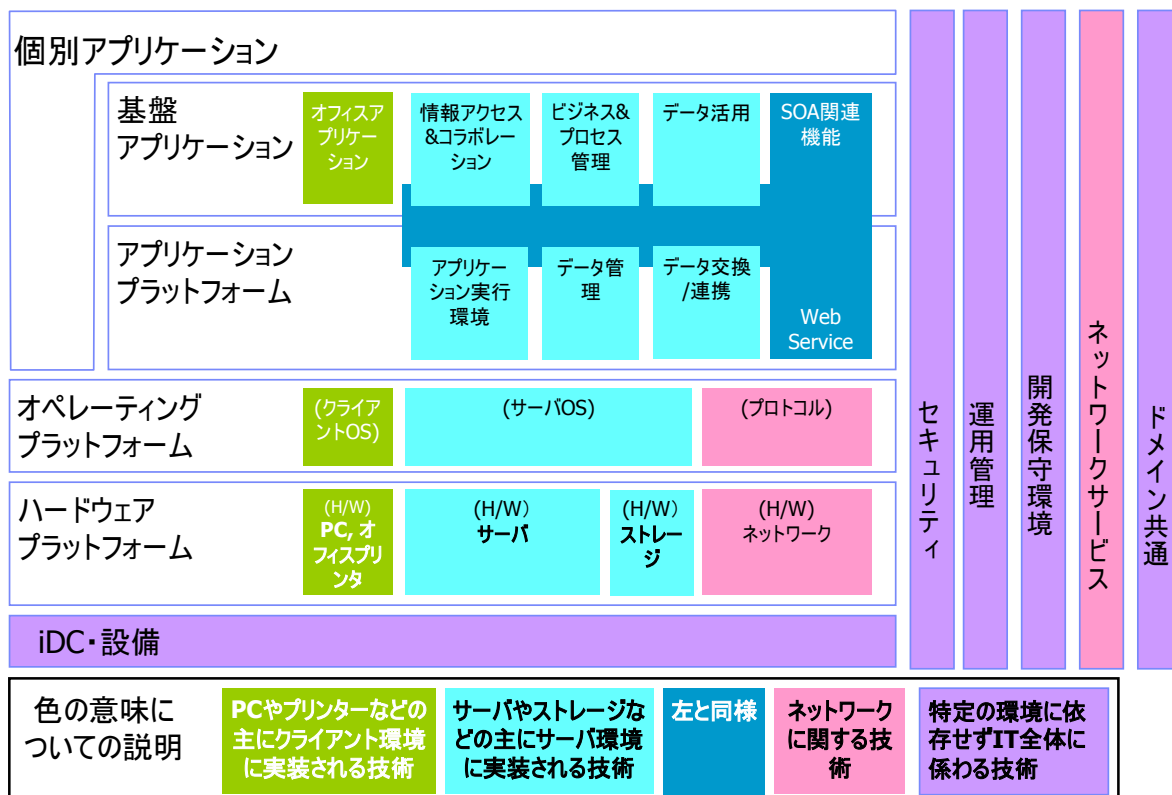



図 3-1 TRM のフレームワーク

参考までに、調達者の視点から同時に調達を行う単位として分割した技術ドメインを、TRM のフレームワーク上の階層図上にマップすると、それぞれの技術ドメインは図 3-2 のような階層に位置する。

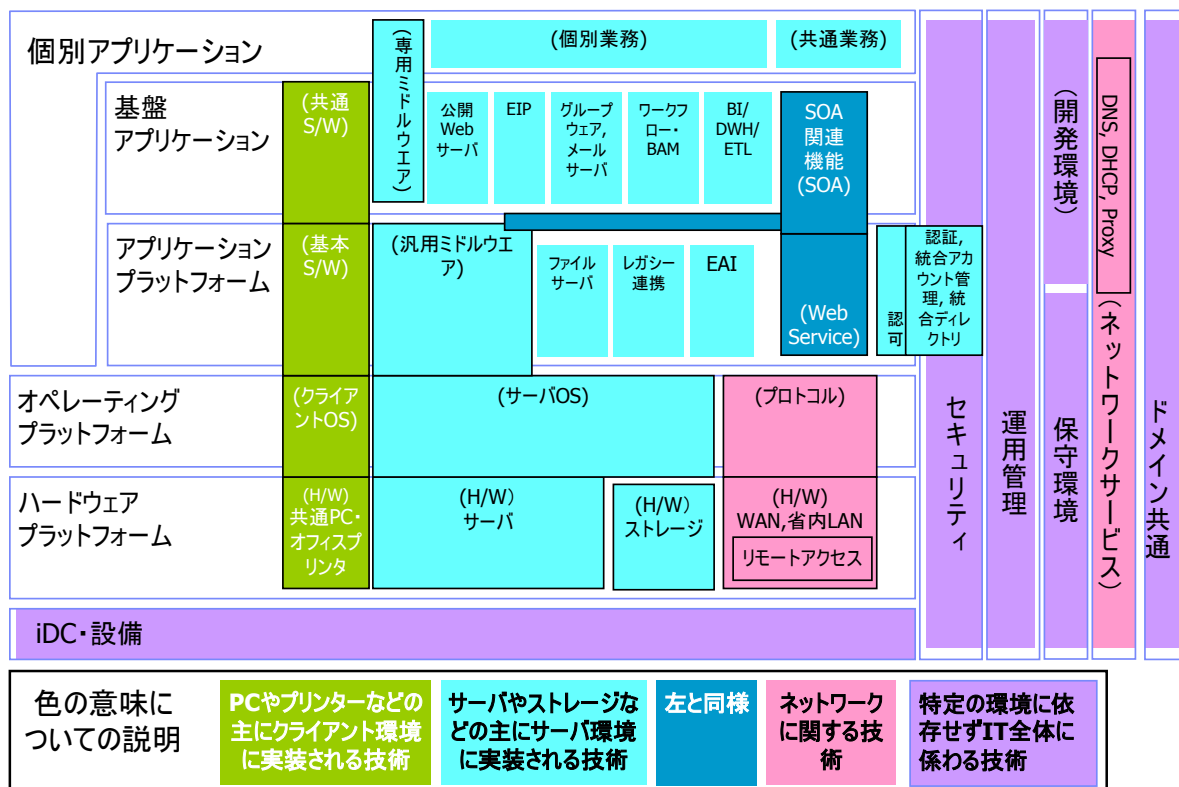



図 3-2 TRM のフレームワークと技術ドメインのマップ

表 3.1 技術一覧表分類

技術一覧表分類			
大分類	中分類	技術 技術ドメイン解説上の相当機能	技術細目
ハードウェアプラットフォーム	PC・オフィスプリンタ	パーソナルコンピュータ	
		シンクライアント	
		オフィス・プリンタ装置	
	サーバ	サーバハードウェア	サーバハードウェア
	ストレージ	ディスクストレージ	
		テープストレージ	
	ネットワーク	LAN	スイッチ
			セキュア無線 LAN
		WAN	ルータ
		リモートアクセス	
		回線サービス	
オペレーティングプラットフォーム	PC・オフィスプリンタ	共通オペレーション環境	OS カーネル
			周辺機器サポート
			コマンドライン環境
			Web ブラウザ
			動画閲覧
	サーバ	サーバ・オペレーティング・システム	OS サービス
		シンクライアントサーバ	
	ネットワーク	DNS/DHCP/Proxy	DNS サーバ
			DHCP サーバ
			Proxy サーバ
		VoIP	
アプリケーションプラットフォーム	アプリケーション実行環境	Web サーバ	
		AP サーバ	
	データ管理	メタデータレジストリ	
		DB サーバ	
		ファイル共有	
		統合ディレクトリ	
	データ交換/連携	EAI	
		アダプタ	
		レガシー連携	

	Web Service	エンタープライズ・サービス・バス	
		Web サービスプロトコル	基盤技術
			セキュリティ関連サービス
			高信頼性メッセージ関連サービス
			トランザクション関連サービス
基盤アプリケーション	情報アクセス&コラボレーション	マッシュアップポータル	
		EIP	ポータルサイト
			パーソナライズ
			アプリケーション統合
		コンテンツ・マネジメント・システム	
		グループウェア	
		電子メール	
		インスタント・メッセージ	
		全文検索	
		Web 会議	
		画面共有サービス	
	ビジネス&プロセス管理	ビジネス・プロセス管理	
		ビジネス活動監視 (Business Activity Monitoring)	
		ビジネスモデルシミュレーション	
		ワークフロー	
	データ活用	ビジネスインテリジェンス	
		データウェアハウス	
		ETL (Extract/Transfer/Load)	
		データマート	
		OLAP (Online Analytical Processing)	
		ODS (Operational Data Store)	
		データマイニング	
		ダッシュ ボード	
		レポーティングツール(レポーティングサービス)	
	SOA 関連機能	マネジメント	
		サービス・リポジトリ/レジストリ	
	オフィスアプリケーション	オフィスアプリケーション	画像処理
			文書作成
			プレゼンテーション

			表計算
			ファクシミリ
			画像パブリッシング
			文書処理
			計算
運用管理	運用管理	運用管理	稼動性能管理
			クライアント PC 管理
			サーバ管理
			ネットワーク管理
			ストレージ管理
			サービスデスク
セキュリティ	セキュリティ	セキュリティ管理	証跡管理機能
			ウイルス対策機能
			ウイルスゲートウェイ
			インターネットコンテンツフィルタリング機能
			ファイアウォール機能
			侵入検知・防止機能
			ネットワーク接続監視機能
			暗号化機能
			スパムメール対策機能
		統合アカウント管理	
		デイレクトリ連携	
		OS アクセス制御	
		Web シングルサインオン	
		デスクトップ・シングルサインオン	
ドメイン共通	ドメイン共通	文字符号	
		グラフィックフォーマット	
		CD-ROM フォーマット	
		DVD フォーマット	
		キャラクタシンボル	
		タグセット/マークアップ言語定義	
		データエレメント標準	
		動画フォーマット	
		圧縮／アーカイブ	
		磁気テープ出力	

		業務情報	
		地図情報	
		キャラクタセット／データ表現	
		ロケール／ネイティブ言語支援	
		プログラミング言語	
		モデリング支援	
		アクセシビリティ	
ネットワークサービス	ネットワークサービス	通信プロトコル	
		タイムサービス	
開発保守環境	開発保守環境	開発環境	
		開発ツール	
		構成管理・バージョン管理ツール	
		プロジェクト管理ツール	
		テストツール	

個別技術	個別技術	ビデオ処理	
		音声情報処理	
		CAD（Computer Aided Design）	
		エキスパートシステム	
		eラーニング	
		キオスク	
		モバイル装置	
		物品情報	
		モバイル／ワイヤレス	
		IC カード	
		メディア配信サービス	
		地図情報サービス	
		文書管理サービス	

TRM 周辺技術	TRM 周辺技術	IT サービスマネジメント	
		ソフトウェアライフサイクル管理	
		IT 内部統制フレームワーク	

4.調達パターンとモデル及び情報システム設計の指針

4.1.機能構成モデル

機能構成モデルにおいては、アプリケーション、共通基盤、ネットワークを構成する諸技術要素を技術ドメイン単位に整理し、各々が提供する機能・サービスを主として調達の観点から整理する。特に、共通基盤とネットワークの境界については、ネットワークにおける諸技術要素を現状の調達実態にできるだけ沿うように定義した。また、本機能構成モデルはプライベートクラウド(プライベート・クラウドとは、自組織内に閉じて構築・利用されるクラウドを指す)環境としての構成要素を含む。

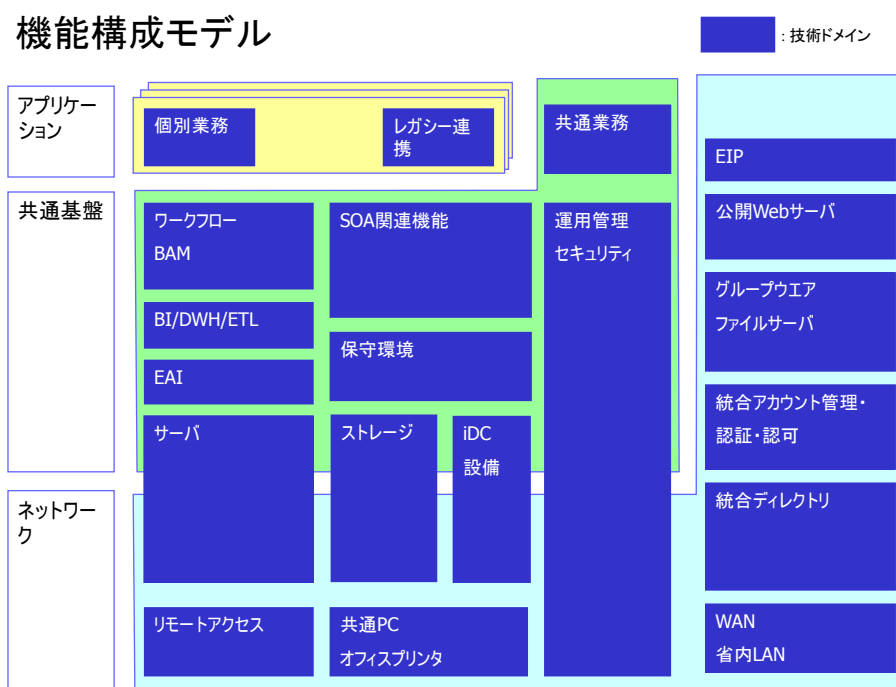



図 4.1-1 機能構成モデル

4.1.1.技術ドメイン定義

技術ドメインは中央省庁の一般的な調達単位に合わせて、諸技術を分類した大項目であるが、複数のドメインにまたがる技術・製品、厳密な定義が困難な技術・製品が存在するため、緩やかな分類を行う大項目として定義される。

以下に各技術ドメインの定義を記述する。

アプリケーション	
技術ドメイン	定義
個別業務	・ 実務手引書で規定されている個別業務 ・ 個々の業務アプリケーション
レガシー連携	・ レガシーシステムで実現した業務と共通基盤上の業務を連携させるためのアプリケーション層の仕組み ・ ただし、EAI 等は除く。

共通基盤	
技術ドメイン	定義
共通業務	・ 実務手引書で規定されている共通基盤システムが提供する共通的な業務 ・ 個別業務から利用される共通的な業務サービス
ワークフロー・BAM	・ 業務プロセスを制御・管理するための汎用的な仕組み ・ ただし、Web サービスをベースとする BPM は除く。
BI/DWH/ETL	・ データ参照・検索・分析を統合的・汎用的、高度に行うことで業務画面や帳票の作り込みを削減するのに役立つ仕組み ・ また、データ操作のための汎用的な仕組み
EAI	・ 業務システム間の連携を汎用的に行う仕組み
SOA 関連機能	・ Web サービスの利用を前提に Web サービスなどを連携させシステム全体を構築する仕組み ・ またそれを支える Web サービス関連技術標準
運用管理・セキュリティ	・ 共通基盤・ネットワークやアプリケーションの運用管理・セキュリティに資する仕組みのすべて ・ ただし、アプリケーションで個別に実装すべき部分は除く。
保守環境	・ アプリケーションや共通基盤の保守に必要な環境を構成する仕組み ・ 特に、本番環境も含めた保守プロセス、開発ツール、自動検証の仕組み
サーバ	・ 上述の機能を支えるサーバ(ハード・ソフト) ・ 信頼性、可用性、柔軟性を備え、一元的に管理される統合環境であり、仮想化されることも期待される。 ・ ルータ/スイッチ等のネットワーク機器も含まれる。
ストレージ	・ 上述の機能を支えるストレージ(ハード・ソフト) ・ 信頼性、可用性、柔軟性を備え、一元的に管理される統合環境であり、仮想化されることも期待される。
iDC・設備	・ 上述のサーバ・ストレージ群が稼動するための物理的な環境と定

	型的な保守・運用サービス （物理的な環境：立地環境も含めた建物・マシン室・設置エリアと電源・空調・通信回線・消火・セキュリティ等の設備）

ネットワーク	
技術ドメイン	定義
EIP	・ 省内向けの統合的なポータルサービス ・ グループウェア機能は原則として除くが、ポータルによる情報発信・共有の仕組みは含む。
公開 Web サーバ	・ 外部向けの公開ホームページ ・ 静的に情報を公開するだけでなく、CMS 等による統合的なコンテンツ管理機能も期待される。 ・ また、簡易的な情報収集・受け付け機能も期待される。
グループウェア・ファイルサーバ	・ メール、スケジュール、会議室・設備予約等のグループウェア機能と簡易な情報共有の仕組み ・ ポータルをベースとする場合は EIP と重複する部分が生ずる。
統合アカウント管理・認証・認可	・ 利用者を統合的・汎用的に管理する仕組み ・ 全利用者にユニークな ID を賦与し、本人認証とアクセス制御を行う。
統合ディレクトリ	・ 上述の統合アカウント管理・認証・認可の基礎となるメタディレクトリ ・ 職員マスター等と基礎データで連携し、ほかの様々なシステムで実装・利用される諸ディレクトリの親ディレクトリとしての機能が期待される。
WAN・省内 LAN	・ 物理回線、 DNS/DHCP/Proxy 等を含めたネットワークサービスの本体 ・ 基礎的なネットワークセキュリティ機能も期待される。
共通 PC・オフィスプリンタ	・ 汎用的な PC とオフィスプリンタ ・ 共通的でセキュアな環境を構築・維持する仕組みを含む。 ・ 特定の業務のみに使用する専用機器は除く。
リモートアクセス	・ 省外から省内 LAN にリモートアクセスするための仕組み ・ ネットワーク接続環境に加えて VPN や認証等の追加的なセキュリティシステムが期待される。

4.1.2.想定される調達対象

また、各技術ドメインが想定する調達対象について、役務と物品とを分けて以下に示す。役務については設計・開発作業を中心に記述している。運用・保守、移行、設置等の作業が別途発生するので留意されたい。

図 4.1-2 調達パターン ― 技術ドメインから見た役務

調達パターン - 物品

図 4.1-3 調達パターン ― 物品

4.1.3.調達における各技術ドメイン要否の考え方

前述の機能構成モデルや調達パターンは必ずしも固定的なものではない。実際の調達においては、共通基盤、ネットワークともに、前述の一覧から必要としないものを削除し、不足するものを追加する必要がある。以下に調達における各技術ドメイン要否の考え方を技術ドメインごとに記述する。

アプリケーション	
技術ドメイン	各技術ドメイン要否の考え方
個別業務	・ 必須
レガシー連携	・ 選択的(可能性：小) ・ 通常は個別業務の作り込みや、EAI・外部連携でカバーされることが多いが、レガシー連携に特化した専用ツールを複数の個別業務で共有することを前提に導入する際には必要。

共通基盤	
技術ドメイン	各技術ドメイン要否の考え方
共通業務	・ 選択的(可能性:大) ・ 詳細は「4.3 業務アプリケーションの考え方」を参照。
ワークフロー・BAM	・ 選択的(可能性:小) ・ ワークフローツール(BPM を除く)については、複数の個別業務での共有を前提に、共通基盤での実装を検討する。 ・ BAM については各府省での業務要件に依存する。
BI/DWH/ETL	・ 選択的(可能性:中) ・ 複数の個別業務での共有を前提に共通基盤で実装するよりも、個別業務での個々の実装に依存する方が合理的な場合も多い。
EAI	・ 選択的(可能性:中) ・ SOA 関連機能でカバーされる場合もある。
SOA 関連機能	・ 選択的(可能性:大) ・ 詳細は「4.4 業務アプリケーションの考え方」を参照。
運用管理・セキュリティ	・ 必須 ・ ただし、調達範囲は要検討。
保守環境	・ 必須 ・ ただし、調達範囲は要検討。
サーバ	・ 必須 ・ 既存資産の流用、外部リソースの活用も視野に入れて調達範囲を検討する。 ・ AP サーバ(ソフト)については個別業務側での調達も視野に入れる。
ストレージ	・ 選択的(可能性:中) ・ 小規模構成の場合はサーバに包含される可能性が高い。
iDC・設備	・ 必須 ・ ただし、庁内設置・外部 iDC 等の選択も含めて調達範囲は要検討。

ネットワーク	
技術ドメイン	各技術ドメイン要否の考え方
EIP	・ 選択的(可能性：中) ・ グループウェア・ファイルサーバでカバーされる場合もある。
公開 Web サーバ	・ 選択的(可能性：中) ・ 別調達となる場合も多い。
グループウェア・ファイルサーバ	・ 選択的(可能性：大) ・ 別調達となる場合もある。
統合アカウント管理・認証・認可	・ 選択的(可能性：中) ・ 共通業務、個別業務、その他調達でカバーされる場合もある。
統合ディレクトリ	・ 選択的(可能性：中) ・ 統合アカウント管理・認証・認可、その他調達でカバーされる場合もある。
WAN・省内 LAN	・ 必須
共通 PC・オフィスプリンタ	・ 選択的(可能性：大) ・ 別調達となる場合もある。
リモートアクセス	・ 選択的(可能性：中) ・ 各府省の要件に依存する。

また、後述「4.4 業務アプリケーションの考え方」で紹介している、パッケージ製品・ミドルウェアについては、個別業務に閉じて調達すべきか、複数の個別業務での共有を前提に共通基盤として調達すべきか等の検討が必要である。CRM、RIA 等については個別業務での調達を前提として共通基盤には含めていないが、共通基盤に含めるという選択も個々の調達においては可能である。

パッケージ製品・ミドルウェアの調達仕様については、「5. 技術ドメイン解説」の記述を利用されたい。「基本」は標準的な製品に期待される機能であり、十分な機能を有しない製品の排除に有効となる。「加点」は各調達対象システムにおいて、必要、もしくは有効と思われる項目に利用されたい。特に、分離調達の対象となるような大規模システムにおいては、拡張性や運用・管理の自動化の観点から、「加点」から必須とすべき項目がないか、十分に考慮されたい。逆に小規模なシステムについては、「基本」であっても機能、性能、信頼性等の観点からオーバースペックとなる可能性があり、安易に必須と指定しないように留意されたい。

4.1.4.調達単位の考え方

調達単位については、役務と物品を分離することが前提となる。ただし、ハードウェアの設置・据えつけ、特段の設計作業を要しないソフトウェア製品のインストール作業等は、物品調達の付帯作業とし、分離させる必要はない。また、ハードウェア保守、ソフトウェア製品保守についても、物品調達に含める。

ただし、小規模案件において、保守体制の単純化に十分な合理性がある場合、もしくは調達手続きの簡素化の効果が期待できる場合は、役務と物品を分離しない選択肢も有効である。

・ 役務調達

役務調達の単位については、設計・開発フェーズ、保守・運用フェーズで分けて考える必要がある。以下は分離調達対象の案件を前提に記述するため、その他の案件は適宜、参考とされたい。

設計・開発フェーズにおいては、まず、個別業務と共通業務に分離されるが、特に共通業務においては、技術ドメインにおける共通基盤の全要素を原則として一つの調達単位と考えるべきである。そして、専門的に特化した技術の必要性から分離させるべきドメインのみを別調達として分離独立させるべきである。この場合、分離独立させる対象は可能な限り必要最小限にとどめ、設計・開発フェーズにおけるベンダー数が安易に増大しないよう、特に留意が必要となる。また、分離独立させる対象は、技術ドメインを単位としつつ、柔軟に対処することが望ましい。

保守・運用フェーズにおいては、まず、保守と運用を分離することが重要となる。ここでの保守とは、そのシステムについての十分な知見を有したベンダーが行う、障害対応や機能追加、改修、チューニング等の作業を指し、運用とは特段の知見を有さないベンダーがマニュアルに基づいて行う、システム監視、障害の一次切り分けやバックアップ等の作業を指す。ハードウェア保守やソフトウェア製品の保守については、物品調達の一環として調達されるものであり、ここでは扱わない。

保守については、原則として設計・開発フェーズにおける設計・開発ベンダーが保守を継続することが基本となる。ただし、多くのベンダーにサポートされるパッケージ製品と最小限の開発量によるシンプルな構成であり、かつ、特段のチューニングを要さないシステムについては、設計・開発ベンダー以外についても検討の余地がある。特に共通基盤については技術要素が多岐にわたるため、特定技術に特化した専門ベンダーの追加の必要性を検討するとともに、共通基盤全体の保守を統括する機能も必要となる。この保守の全体統括機能については、共通基盤の中心ベンダーの分担とすることを基本とするが、その他の可能性についても検討の余地がある。

運用については、設計・開発ベンダーに依存する必要がないため、設計・開発時や保守の調達単位を単純に踏襲せず、可能な限り統合することを推奨する。

・ 物品調達

物品調達の単位については、可能な限り集約して調達数の削減を図ることが好ましいが、特殊な製品、調達時期の異なるもの、設計の変更や見直しによって契約変更の可能性が高いものについては、別調達とすることが実際的である。

4.2.物理構成モデル

物理構成モデルは、調達仕様書を作成する際に、情報システムの全体構成を考える上で参考となることを目的に作成された。システム構成としていろいろな形が考えられるが、ここでは、現在の府省庁での調達で特に役立つと思われる「ネットワーク」と「共通基盤」の 2 種類について、各省庁内で一般的と考えられる具体的なシステム構成イメージを示した。

この構成モデルは、物理的な構成を表した図ではあるが、あくまでも一例である。構成モデルに書かれたすべての要素について、必ずしも物理的に別々に用意する必要はない。複数の要素を同一ハードウェア上に実現可能な場合や、既にある資源を利用可能な場合も考えられる。調達時には、案件ごとに必ず最適化の視点、既存資源活用の留意点等を総合的に考慮した上で、システム構成を個別に検討する必要がある。

ネットワーク物理構成モデルとは、各省庁内ネットワークの全体構成イメージを示したものであり、共通基盤物理構成モデルとは、ネットワーク物理構成モデル上の各種サーバについて、共通となるようなシステムの基本構成を示したものである。

ネットワーク物理構成モデルは、CIO 補佐官等連絡会議の第 4 ワーキンググループ(情報セキュリティ)の 2006 年度成果物をもとにしている。各省の最適化計画を参考に、府省内ネットワークをモデル化して、S1～S6 の 6 つのセグメントに分類した。セグメントはそれぞれ、S1 は DMZ、S2 はイントラ用サーバセグメント、S3 は本省 LAN、S4 は本省内外各種サーバセグメント、S5 はネットワーク、S6 は遠隔・持ち出しを示している。

図 4.2-1 ネットワーク物理構成モデル

共通基盤物理構成モデルとは、各省庁内のシステムについて、各種サーバを中心に描いた構成イメージである。共通基盤基本機能とは、各省庁で共通的に必要なシステムの基本機能であり、ネットワークアクセス、利用者登録・認証、共通データベース管理(選択)、個別アプリケーションとの API・プロトコル、他システム連携(選択)、共通セキュリティ基盤、運用・保守基盤、共通アプリケーション(選択)、共通公開ポータル(選択)、共通リポジトリ等が考えられる。((選択)とは、オプショナルな機能を意味している。)

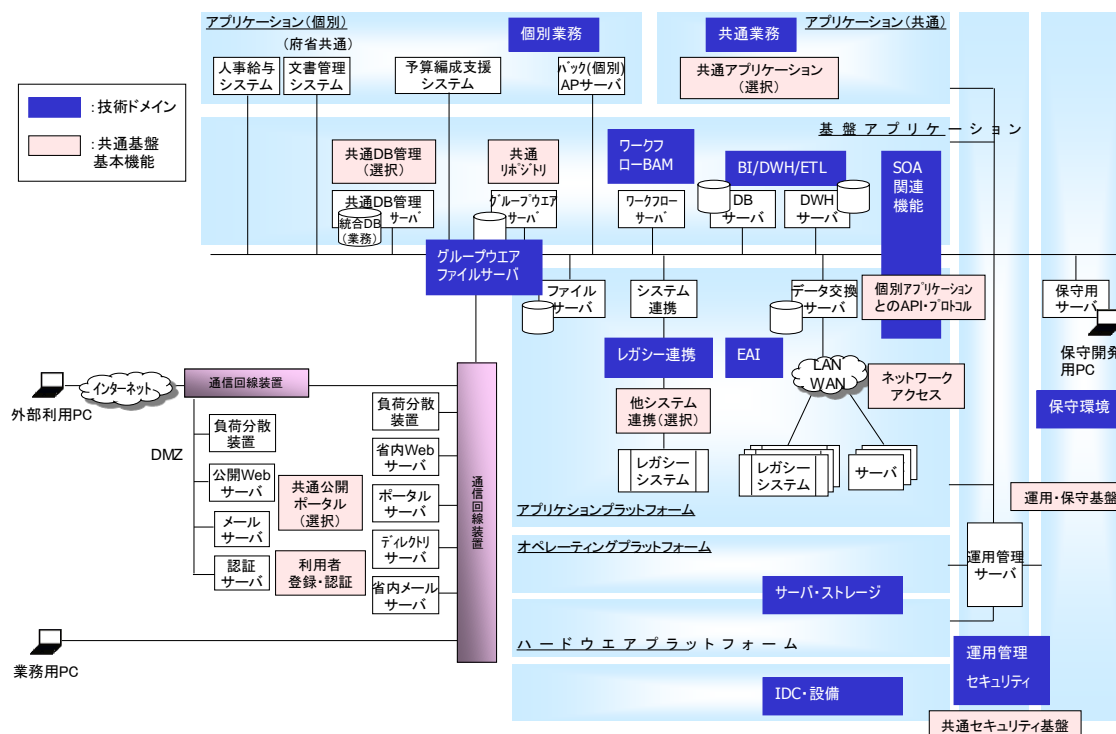



図 4.2-2 共通基盤物理構成モデル

4.3.役務の分類

機能構成モデルの各技術ドメインは物品の調達に視点を置いたものであるが、役務を調達するときは情報システムの調達フェーズに沿った分類を考えるとわかりやすい。調達フェーズは企画から始まり、要件定義、開発、運用・保守と進む。主要な役務と情報システムの調達フェーズの関係を図 4.3-1 に示す。各役務の内容と仕様書記載のポイントは 6 章に示されている。

図 4.3-1 役務調達の分類

システム構築は、設計、開発、テスト、移行の各詳細フェーズから構成され、運用･保守へと続く。さらに、システム構築は、全く新規に開発する場合(新規開発)、古いシステムを新しく作り直す場合(システム更改)、ハードウェアの入れ替えに伴ってシステムを載せ替える場合(ハードウェア更改)、サブシステムを追加して機能を追加する場合(機能追加)、などがある。また、アプリケーション保守の中にはアプリケーションの一部改修･機能追加を役務として含む場合(改修)がある。図 4.3-2 にこれらの関係を整理した。役務作業として設計プロセス(基本設計･詳細設計)を含む役務調達に関しては6.3.システム構築(設計･開発)に、設計プロセスを含まない(設計書の修正レベルは含む)役務調達に関しては 6.6.保守の中の 6.6.3.アプリケーション保守に分類している。詳細な解説は 6 章を参照されたい。

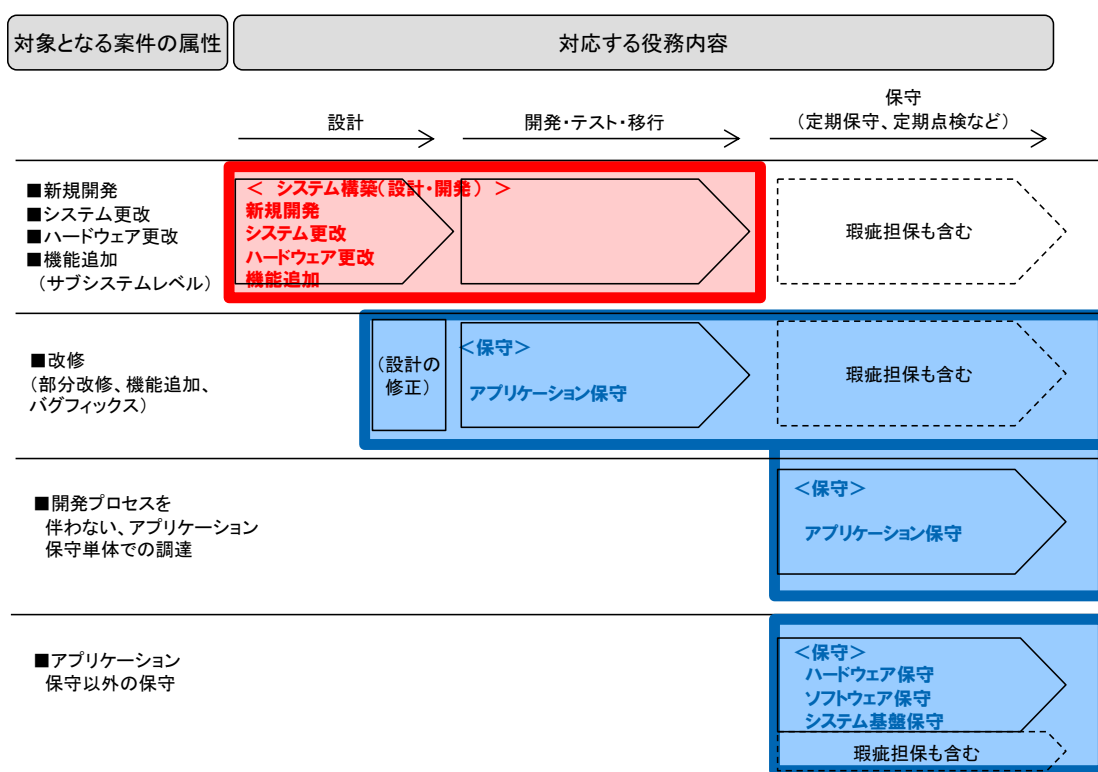



図 4.3-2 システム構築(設計･開発)とアプリケーション保守の対応関係

役務の分類を機能構成モデル調達パターンの役務との関係で示したのが、図 4.3-3 である。開発フェーズで見ると機能構成モデルの役務で示すほとんどの役務はシステム構築に分類されるが、ネットワーク調達やiDC設備調達付帯作業はそれぞれの役務に独立して分類される。サーバ調達やストレージ調達については設計・構築はシステム構築の役務となるが、導入・設置は機器調達付帯作業として分類される。運用や保守については運用・保守フェーズで調達される。図 4.3-3 では企画フェーズと要件定義フェーズは省略している。

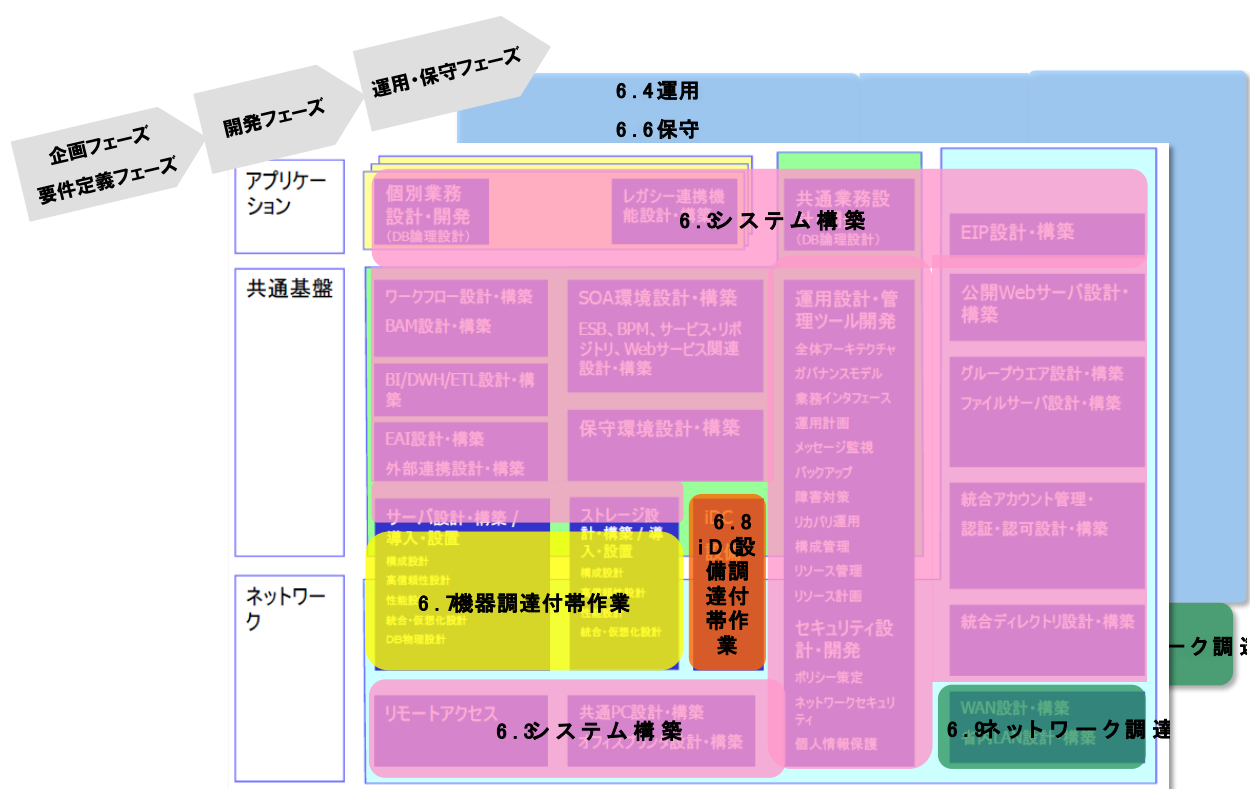



図 4.3-3 機能構成モデル 調達パターンー役務 との対応関係

4.4.業務アプリケーションの考え方

機能構成モデルのアプリケーション、共通基盤において各々定義されている個別業務と共通業務については、実務手引書で規定されているところであるが、共通業務については、大きく以下の 3 種類の考え方が混在している。

A: 電子決済等、特定の具体的な業務であり、上位の業務レイヤーに属するもの
B: BPM 機能や BI 機能のように共通基盤が提供する諸システム機能
C: SOA でいうところの上位サービスから呼び出される下位の共通サービス

共通業務と個別業務の境界定義、より具体的には共通業務のくくり出しについては困難と目されているところであるが、Aについては比較的明解であり、具体的な業務の範囲と機能・仕様を明確にした上で、個別業務からの利用インタフェースを規定すればよい。

B については共通基盤が提供する諸システム機能に対するイメージが共有されていないために生じている混乱であり、本技術参照モデルによって共通基盤の提供する諸機能への理解が共有されることで、混乱が解消されることを期待したい。共通基盤を導入して共通基盤上で業務アプリケーションを稼動させるのであれば、共通基盤で用意されている様々な機能を十全に活用する姿勢が不可欠である。共通基盤の機能を活用することによって、開発量を削減し、プロジェクトのリスクと開発コスト・アプリケーションの保守コストを削減することが期待されている。

C については、SOA でいうところのサービス粒度や共通サービスの定義・くくり出しに大きく依存する領域である。しかしながら、現状では SOAや SaaS 等の技術の普及・浸透は十分でなく、その適用への過渡期であるため、最終的な解決までには相当の時間が必要と考えられる。特にCについては、後述の段階的なアプローチの一環と位置づけ、共通業務として共通基盤開発業者が整備するよりも、個別業務内に閉じて個別業務開発業者が開発する形態を第 1 段階としては推奨する。

以下、これらを前提とした業務アプリケーションの考え方を記述する。

4.4.1.段階的なアプローチと全体アーキテクチャの見直し

共通業務、特に前述 C の共通サービスを定義する上での一つのポイントが段階的なアプローチである。プロジェクトが大規模で長期間のウォーターフォールモデル型となる場合、共通業務の範囲と機能・仕様はあらかじめ厳密に定義されるべきである。すなわち、BPRを包含した業務分析を行い、業務の上位概念から個々の詳細レベルのビジネスプロセスまでが ToBe 的にブレークダウンされていることが前提となる。現行業務システムの AsIs 的な処理フロー、業務画面等からの単なる焼き直しでは、レガシーシステムを再開発するだけとなってしまう。

しかしながら、多くの場合、このアプローチは困難であり、さらに SOAや SaaS 等の技術の普及・浸透が十分でない現状では、関係者の技術力、経験も含めて困難である。

従って、まずは大規模で長期間のウォーターフォールモデル型となるプロジェクトの規模を縮小させること

が重要となる。規模を縮小させた上で段階的なアプローチをとることを推奨したい。

システム化対象の縮小や業務機能の削減は別として、プロジェクト規模の縮小には大きく 2 つの手法がある。

一つはプロジェクトの分割、すなわち開発期間と費用を見据えたスコープの適切な分割である。業務システムを疎に連携可能な単位に分割し、サブシステム間を EAI 的な手法で連携させる方法である。もちろん、DOA(データ中心)をベースに統合的なDBを中心に置き、その周辺にアプリケーション群を配置することで、サブシステム単位にプロジェクトを分割するのも有効な方法である。いずれにしても、この手法をとる場合には全体アーキテクチャの策定・見直しが必須となる。現状のサブシステム単位をベースとした調達単位の単純な分割とはならないため、特に注意が必要である。

2 つ目は後述のパッケージ製品の適用による開発量の抜本的な削減である。もちろん、プロジェクトの分割と開発量の抜本的な削減は併せて検討されるべきものであり、その前提として全体アーキテクチャをきちんと定義することが重要である。

このようにプロジェクトの規模を縮小し、開発量を削減することで、段階的なアプローチをとることが可能となる。段階的なアプローチの初期においては、大きな粒度のサービスでシステムを構成し、各サービス間を EAI 的に疎に連携するところから着手すべきである。その後、段階的にサービスを分解し、サービス粒度を小さくしていく過程で共通サービスを具体化させることが望ましい。

また、段階的なアプローチは設計から運用までの 1 回の流れの中でインクリメンタルに実行される場合と複数回の流れの中で長期的に実行される場合の双方を想定することが望ましい。

段階的なアプローチの実現には、最初に、全体アーキテクチャの策定、及び、共通基盤とパイロット業務を中心とした実証実験やプロトタイピングが必要であり、この作業は、以下のいずれか、もしくは組み合わせによって実施される必要がある。

・企画段階で CIO 補佐官の助言を得ながら職員が行う。

・全体アーキテクチャ策定や実証実験・プロトタイピングを行う事業者を調達する。

・共通基盤システム事業者が受注後に、「基本的事項の整理」において行う。

そして、段階的なアプローチを通じて、システムが段階的に整備され、全体アーキテクチャについても維持と見直しが必要となる。いずれにしても、本技術参照モデルが活用されることにより、全体アーキテクチャ策定や後続の作業が円滑に実施されることが期待される。

4.4.2.パッケージ製品等の適用による開発量の抜本的な削減

公共システムにはコンピュータの黎明期よりシステム化され、当時のシステムアーキテクチャを現在にまで踏襲しているシステムも少なくない。

開発量の抜本的な削減には、カスタマイズせずに適用可能な業務パッケージが存在することが理想ではあるが、府省の業務には難しい場合が多い。しかしながら、汎用的なパッケージ製品、ミドルウェア製品、インターネット関連技術には府省の業務システムにも適用可能な製品・技術が少なくない。

ターゲットとなる業務にフィットする業務パッケージが存在する場合は、そういった業務パッケージ製品を適用することを前提とした上で、最適な業務パッケージ製品が存在しない場合においても、パッケージ製品の適用によって開発量を削減可能と思われる方法を以下に例示する。

・ ケース管理業務における CRM 製品の活用

CRM 製品とは民間企業において、顧客管理に利用されるパッケージ製品である。顧客ごとにどのような属性をもち、どのような取引履歴があり、どのような営業活動を行い、クレーム等も含めて、そこにどのようなコミュニケーションがあり、どのような対応をしたかを総合的に管理する。

公共システムにおいても、国民や企業単位に上記のような事象(ケース)を管理する業務には CRM 製品が適用可能である。公共分野でのケース管理の例としては、税や保険関連の業務が想定され、これらの業務システムのエンジンとしての適用が考えられる。

・ 台帳管理業務における表計算ソフトの活用

台帳を管理する業務については、表計算ソフトで電子的に台帳イメージを作成することが好ましい。複数のオペレータが存在する場合や、表計算の能力を超える件数を扱う場合には、フロントエンドに表計算ソフトを置き、バックエンドに RDB を置き、両者を SQL や Web サービスで連携させる。連携のためのミドルウェアを使うことも有効である。

・ 参照・検索・分析、帳票印刷、統計処理における BI ツールの活用

ケース管理業務や台帳管理業務、もしくはそれ以外のシステムにおいても、データの参照・検索・分析、帳票印刷については、BI ツールを適用することで開発量を大きく削減することが可能となる。特に統計業務については開発量の削減に加えてデータマイニング等の機能が業務改善に期待できる。

・ 画面プログラムにおける RIA 技術の活用

メインフレーム時代の画面プログラムにおいては、もろもろの技術的な制約によって、1 画面に表示できる情報が少なく、そのためにシステムの都合で業務画面を細分し、複雑な業務メニューを構成せざるを得なかった。また、C/S システムで比較的、リッチな画面を使用者に提供していた業務システムが、安易に Web システム化されると、ブラウザを画面として使用する制約から情報量や使い勝手が犠牲にされることも懸念された。

しかしながら現在においては、Ajax 等の RIA 技術を利用することで、豊かな情報量と優れた使い勝手を Web システムでも提供可能となっている。これにより、画面数を削減し、開発量が削減されるだけでなく、利用者の操作性・作業効率と満足度の向上、保守コストとトレーニングコストの削減も期待される。

また、RIA 技術はインターネット上の諸サービスとの連携にも優れており、インターネット上の地図情報や書誌情報等を低コストで活用することにも有効である。

・ 画面プログラムにおける SOAP インタフェースを有する PC 用パッケージ製品の活用

SOA を適用した業務システム構築の考え方として、サーバ側で様々な機能を Web サービスとして提供し、クライアント PC 上の SOAP インタフェースを有するパッケージ製品が前述の Web サービスをサービスコンシューマとして利用することで、利用者の個別要件にフィットする自由度の高い画面プログラムを比較的、小さな開発工数で提供することができる。

対象となる PC 用の製品には、表計算ソフト等の OA ソフト製品、メーラー、及び本用途向けの専用製品等が想定される。また、サーバ側の Web サービス提供については、SOA ベースで諸機能が Web サービスで提供可能な製品を用いる場合と、既存の実装に Web サービスインタフェースを追加する場合が想定される。

・ ワークフロー管理における BPM 製品と統合ディレクトリの活用

りん議・決裁のように複数の担当者(決裁者)の処理を管理する仕組みがワークフロー管理である。ワークフロー管理においては、担当者(決裁者)の情報や、処理ルート(決裁ルート)の管理が負担となる。専用のワークフロー製品を適用する選択肢もあるが、共通基盤で整備される BPM 製品とネットワークで整備される統合ディレクトリを活用することも有効な選択肢である。

・ サービス再利用時の BPM 製品と ESB 製品の活用

サービスを再利用する際には、BPM 製品と ESB 製品の活用を検討すべきである。従来の業務アプリケーションにおいては、諸機能をどのように組み合わせ、どのような分岐条件で処理を進めるかをプログラムや JCL 内にコーディングしており、これが再利用の障壁の一つとなっていた。今後はサービス化した諸機能を BPM 製品と ESB 製品を活用して利用することで、再利用が促進されるとともに、柔軟性とメンテナンス性の高い業務アプリケーションとなることが期待される。

また、SOA のベースとなるサービス指向においては、新たに作ることよりも使われること、再利用されることが重視されており、この考え方に基づいた業務モデル、業務フロー、共通・標準機能等もあらかじめ提供されるようになってきている。これらを柔軟に活用、連携させることにより、リスクと開発量を大きく削減することも期待できる。

・ クラウドサービスの活用

これまで記述してきた諸機能については、パッケージ製品での利用に加えて、クラウドサービスによる実現も視野に入れられる。(クラウドサービスの活用については、4.8 節「クラウド利用者の立場からの考え方」及び 4.9 節「クラウドを構築する立場からの考え方」も併せて参照されたい。)

現在、パブリッククラウドで提供されている機能には、前述の CRM、表計算、BI に加えてグループウェア等があり、今後も急速に発展することが予想されるため、その適用検討は常に行われるべきと考える。

クラウドサービスには、低初期コスト、短期間で利用可能となること、業務ニーズの増減に対応が容易なこと、運用負荷が軽減されること、さらには省エネルギー化等のメリットが期待されるが、その利用に際しては、どのようなサービスの利用が可能か、制度上の制約、セキュリティや BCP、SLA に特に注意を払われたい。具体的には、サービスレベルに関する重要項目(可用性、信頼性、データ管理方法、セキュリティなど)をリスト化し、確認することが望ましい。また、クラウドサービスは、いまだ初期段階であり、国内外共に事例が少な

いこと、これまでの物品調達ではなくサービス調達になること、特にパブリッククラウドについては現時点では選択肢が少ないために新たなベンダーロックインとなる可能性を内包することを、調達の課題として理解しておく必要がある。

4.4.3.パッケージ製品等の適用のための要件定義

業務システムの要件定義の際に、現行システムの機能を、その必要性を再評価せずに、安易に踏襲したり、業務担当者の要望を単純に羅列したりすると、多くの場合、パッケージ製品の適用が非常に困難となってしまい、開発量も膨大なまま削減されない。

こういった事態を避けるためには、要件定義において、パッケージ製品等の適用を強く意識することが必要である。全体アーキテクチャの策定時、業者への見積もり依頼時、調達仕様作成時、設計時のすべてにおいて、真に必要とされる業務要件を、パッケージ製品等を適用していかに合理的に実現するかという視点が不可欠となる。

特に想定するパッケージ製品等が未定の段階においては、本TRMの5章の記述等から一般的な製品のもつ機能を想定して設計を行い、製品確定後に設計を見直す方法を強く推奨する。

4.4.4.段階的アプローチにおけるレビュー

段階的アプローチは前述のようにプロジェクトのリスク軽減や開発規模の削減に有効だが、それに加えてより利用者満足度の高いシステムの構築にも寄与するところが大きい。

従来のウォーターフォール型モデルの場合は、利用者の意見を適宜反映させることが、事実上、困難であった。設計フェーズにおいて、設計ドキュメントでコメントを求めても、実際の業務運用をイメージするのが難しいため、設計時点では有効なコメントが提出されず、実装後に初めてコメントが提出されることが多かった。そして後段のフェーズで提出されたコメントは開発作業に手戻りを発生させるため、プロジェクトを混乱させたり、採用が見送られたりすることも多かった。

段階的なアプローチにおいては、設計フェーズでの実機によるレビューを強く推奨する。全機能、全画面を対象にするのではなく、主要な機能・画面について、設計と同時に実装を行い、利用者に実機を操作した上でのコメントを要求する。そして、実機上で利用者の満足する主要な機能・画面の設計を固め、その後に全体に展開していく。

この実機によるレビューは利用者満足度を高めるだけでなく、後段のフェーズでの手戻り、プロジェクトのリスクを削減し、さらには、実機レビューを容易化するために開発量の削減、パッケージ製品等の適用推進にも大きく寄与することが期待される。

4.5.共通データベースの考え方

全体最適化を指向してシステムを大きく見直す際には、データの見直しも不可欠となる。個別最適化されたデータベース群を見直し、全体最適を指向した共通データベース(以下　共通 DB)を構築することは、システム全体を高度に合理化し、単にコストを削減するだけでなく、より高レベルな行政事務、国民へのサービス提供に大きく資することが期待できる。

4.5.1.共通 DB の定義と在り方

共通 DB については、先進的な府省において検討されているところであるが、大きく以下の 3 種類の考え方が混在している。

最適型共通 DB： 日本政府全体での最適化を志向する共通 DB
中核型共通 DB： 特定府省における中心業務の中核となるデータの共通 DB
参照型共通 DB： 特定府省の特定業務のデータを広範に参照

最適型共通 DB については、企業に関する基礎的なデータや、国民に関する基礎的なデータの集約が期待されるところである。企業については商業登記を基礎情報とした上で財務・税務に関する情報を中心とした全体最適化が望まれ、国民については戸籍等を基礎情報とした上で住民基本台帳等の情報を中心に府省・自治体も含めた全体最適化が望まれるところである。しかしながら、ステークホルダーの多さ、影響の大きさ、個人情報保護等、課題も大きく、本書では扱わない。

中核型共通 DB については、特許庁における特許事務に関するデータ等の例が想定され、特定業務の実施を目的とする府省では非常に重要なデータとなるが、対象となる府省・業務は限定的となる。

参照型共通 DB については、統計データ等の例が想定され、多くの府省で計画・整備の進展が期待されるものである。

共通DBを個別業務と扱うか、共通業務と扱うかは、各府省の考え方に依存するが、複数の個別業務での重複部分を最小とする全体アーキテクチャが要求される。また、特定の府省で整備された共通 DB であっても、その公開・参照利用については、オープンなインタフェースであることを前提に、他府省・自治体・国民等も含めて広範に計画・構築されることが望ましい。

また、人事給与や文書管理等、府省共通システムで整備されることが期待されるデータについては、本書では扱わない。

4.5.2.共通 DB を利用する業務システムの考え方

BI、CRM 等の製品を活用することが前提となる。スクラッチで作り込む場合、もしくは製品にカスタマイズとして追加開発(アドオン)を行う場合には、アプリケーションがデータを囲い込むのではなく、DOA の考え方に基づき、中心に配置するデータの外側にアプリケーションを配置する設計とするべきである。

また、共通 DB の広範な利活用を促進するために、データ更新系のプロセスとデータ参照系のプロセスは

分離して設計すべきである。特にSOAを適用する場合、データ更新系のプロセス(サービス)については、更新したデータをサービスプロバイダとして提供し、そのサービスをデータ参照系のプロセス(サービス)がサービスコンシューマとして利用する設計が推奨される。このようなサービス化されたデータの利用により、共通DBの広範な利活用が促進されるだけでなく、再利用も大きく促進される。

4.5.3.共通 DB の構築事業者と役割分担

DB 物理設計・構築は共通基盤構築事業者、DB 論理設計・構築は個別業務構築事業者が実施することを原則とする。

ただし、共通 DB を個別業務ではなく、共通業務と位置づける場合は、DB 論理設計・構築を共通業務事業者が行うため、すべてが共通基盤構築事業者の担務となる。

運用・保守については、設計・構築を行った事業者に保守を担務させるという選択肢もある。

4.5.4. 共通 DB の計画・導入時における段階的なアプローチ

共通DBは設計も関係者間の調整も困難であることが一般的である。よって、その計画・導入については、実証実験、部分的な導入、全体的な導入と段階的に進めていくことを推奨する。

また、段階的なアプローチの初期の段階では、作業効率を向上させることを目的に、論理設計・構築を行う事業者が物理設計・構築も併せて行う体制・役割分担を推奨する。

いずれにしても個々に DB をもたせるのは保守管理コストの増大等の不都合や拡張性に対しての不整合が発生しやすい。よってできるだけ広範に利用可能な共通 DB を検討することが望まれる。

4.6.府省共通システム導入の考え方

府省共通システムは府省の枠を越え政府全体で全体最適化を指向するものであり、単に導入するだけでなく、府省独自システムの削減と合理化に明確に資することが期待される。

4.6.1.府省独自システムとの連携の考え方

府省共通システムと個別システムとのインタフェースはできるだけシンプルな疎結合とすべきである。これは、通常のシステム間連携においても一般的な考え方であるが、特に府省共通システムは多くのシステムと連携するため、他システムの変更に伴う影響を可能な限り受けにくい形にしておく必要があるためである。疎結合の具体的な連携方法についても、府省共通システム側の用意するインタフェースをそのまま利用し、個別の実装は特段の必要性がない限り避けるべきである。

ワークフローや認証基盤等、府省共通システムで提供される共通的な機能は共通業務の一環ととらえて積極的に活用すべきである。しかしながら、それによって該当機能の府省独自の実装が不要になるわけではない。段階的な適用・導入時において経過的、時限的に必要なだけではなく、ToBe モデルにおいても、府省固有のニーズに対応するためには、府省共通システムを複雑な形で適用するよりも、個別にシンプルな独自実装とした方が合理的となる場合も想定される。いずれにしても、独自の実装については、十分な検討・評価が必要となる。

4.6.2.全体最適をより指向した導入の考え方

府省共通システムの導入については、システムごとに導入の計画、移行作業等が検討されることが多いが、府省共通システムには認証機能やワークフロー機能、職員情報等で相互依存関係が存在する。府省共通システムごとの検討を基本としつつも、全体的な調整・検討を行うことを強く推奨する。

全体的な調整・検討においては、導入スケジュール、データ移行、既存システムとの連携が主要な課題となるが、既存システムやこれから導入されるシステムも含めた、ディレクトリ情報、認証機能の扱い、外字も含めた文字コードの扱い等についても、全体レベルでの調整・検討を行うことを強く推奨する。

4.7.仮想化技術

仮想化とは、IT リソースとそのリソースを利用するユーザ(OS やアプリケーション)との間に抽象化レイヤーを設けることで、IT リソースの物理的性質や限界を隠蔽し、柔軟なリソースの利用を可能とする技術である(図 4.7-1)。1960 年代にメインフレームのハードウェア利用効率を高めるため開発されたのが始まりといわれている。近年、インフラの使用率低下やインフラコストの増加、IT 管理コストの増加、電力使用量の増加等、IT に関連する様々な課題を解決する一つの方法として「仮想化技術」が注目されている。4.7 節では、ハードウェアが IT リソースで、OS をユーザとする仮想化(*1)についての考え方を記述する。仮想化技術を具現化した仮想化機構には、仮想化ハードウェアによる実現と、仮想化ソフトウェアによる実現がある。

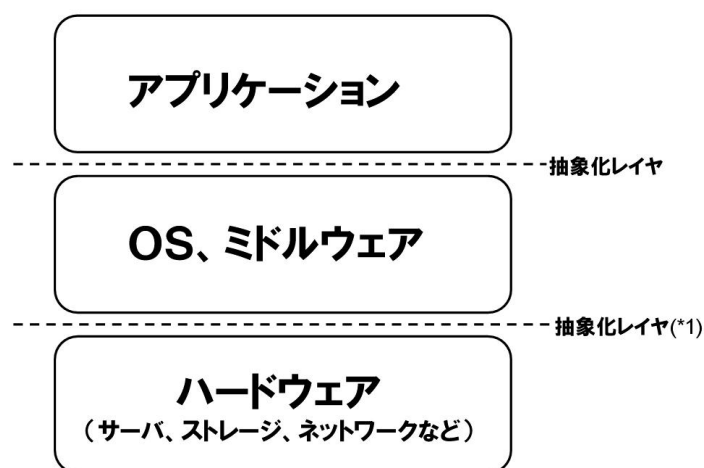



図 4.7-1 仮想化の概念

4.7.1.仮想化技術の利用について

仮想化技術を利用することで、IT リソースを効率的に活用できる可能性がある。また、ハードウェアを仮想化することで、設置スペースの節約、電力使用量の削減、システムの柔軟性が向上することによる運用管理負荷の軽減も期待できる。一方、仮想化することによりシステムのオーバヘッドが増すとか、既に稼動中のシステムを仮想化する場合、アプリケーションを変更なく移行できるとは限らない等の課題もあるため注意が必要である。

4.7.2.仮想化の範囲

・ サーバ仮想化

1 台の物理サーバを複数のサーバがあるかのように使えるサーバ仮想化と、逆に複数台のサーバハードウェアの能力を一つに集約して見せるサーバ仮想化がある。ここでは、主に調達で検討されると想定する前者について記述する。サーバ仮想化ソフトウェアを利用することにより 1 台のサーバハードウェア上に複数の仮想サーバ群を構成することができ、個々の仮想サーバに OS をのせ、それぞれ独立に動作させることができる。1 台のサーバハードウェア上に複数の仮想サーバ群を構成するサーバ仮想化ソフトウェアが仮想マシンモニタ(VMM)である。VMM はハードウェアをエミュレートして独立した仮想サーバ(仮想マシン)を提供する。仮想サーバを “ゲストサーバ”、仮想サーバ上の OS

を“ゲストOS”とも呼ぶ。VMMは、ホスト型VMMとハイパーバイザ型VMMに大別できる(図 4.7-2)。

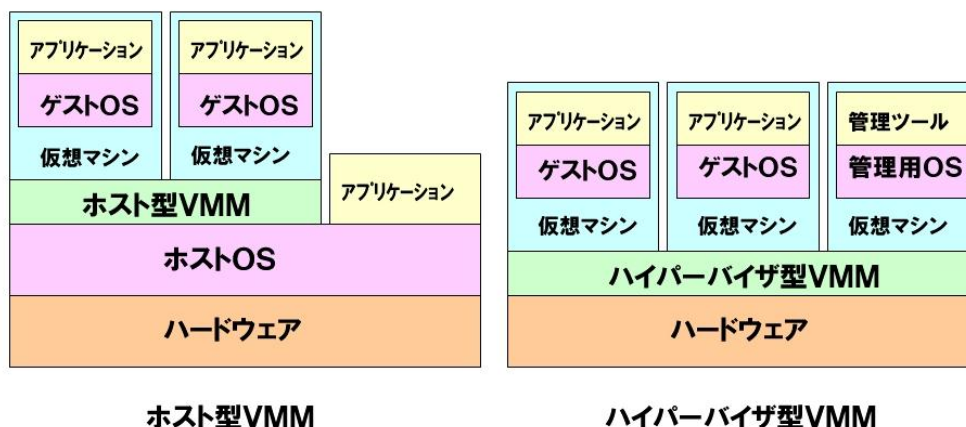



図 4.7-2 サーバ仮想化の2つの方式

・ ストレージ仮想化

ハードディスクドライブ等の一つの物理ストレージを複数の仮想ストレージに見せる「ストレージ分割」、複数のストレージを集約しあたかも一つの巨大なストレージのように見せる「ストレージ統合」、サーバに見せる容量を物理容量から独立させる「ストレージ容量仮想化」がある。RAID でも複数ストレージの統合は実現できたが、「ストレージ統合」ではきょう体をまたがることも可能となった。

・ ネットワーク仮想化

物理的な接続形態とは別に仮想的なネットワークを構成し、端末をグループ化する「VLAN」や、ルータ･スイッチ、ファイアウォール、ロードバランサ等のハードウェアを複数に見せたり、複数の装置を集約して1台に見せる「ネットワーク装置の仮想化」がある。

・ デスクトップ仮想化

アプリケーション処理やデータの保存はすべてサーバ側で行い、クライアントでは画面表示とキーボード･マウス等の入出力処理のみを行うようにする画面転送型シンクライアント技術の一つ。画面転送型を実現する方式として、サーバベースコンピューティング方式、ブレードPC方式、仮想PC方式(VDI 方式)がある(図 4.7-3)。仮想 PC 方式では1台の物理サーバ上に複数の仮想マシンを設定し、それぞれの仮想マシン上で各クライアントの OS、アプリケーションを動作させる。

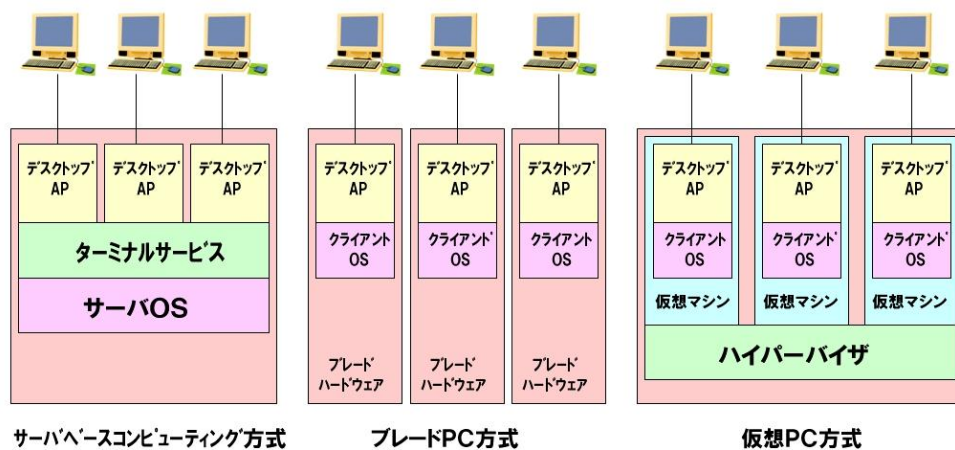



図 4.7-3 デスクトップ仮想化の3つの方式

4.7.3.仮想化構築時の留意点

仮想化技術を利用してシステムを構築する際に考えておかねばならない留意点を挙げる。

- 従来の各 H/W 資源単位でのサイジングに対し、仮想リソースの割当単位、業務システムの単位、物理リソースの単位、リソースプールの単位に分けて検討する必要がある。
- 従来 H/W 層で、1:1 もしくは N:1 などのモデルで設計していたサーバの高可用性要件について、他の高可用性要件を考慮した上で、仮想化層において、リソースプール全体での N:M モデルの適用を検討する。
- ハイパーバイザ、仮想サーバ、クラウド管理層の監視とセキュリティ、複数の仮想資源の構成管理は、従来のシステム設計に追加して検討が必要である。
- 仮想化によるパフォーマンスの低下、リソース管理の不可視(見えにくくなる)、マルチテナントでのリソース競合に注意を要する。
- 調達するハードウェアが利用したい仮想化機構に対応しているか確認が必要である。
- 利用したいソフトウェア(プログラム)が仮想環境に対応するか確認が必要である。
- 仮想化に移行する場合、特にデバイスドライバ関連で必ずしもネイティブと同様に動作するとは限らない。
- 物理環境から移行する場合、移行計画(サイジング、動作検証、データ移行、など)が必要である。

4.8.クラウド利用者の立場からの考え方

クラウドとは、一般的に「ネットワークを通じて、情報処理サービスを、必要に応じて提供／利用する」形の情報処理の仕組みを指し、利用者としてクラウドより提供されるサービスを利用するという観点と、自らクラウドを構築して、クラウドサービスを提供するという観点の双方が必要となる。本節においては、クラウドより提供されるサービスを利用する観点から、クラウド利用者が考慮すべき点を記述する。

4.8.1 クラウドサービス選択の基本的な考え方

クラウドには様々な形態があるが、まずは、利用対象がオープンになっているか否かによって、パブリッククラウド、プライベートクラウドに大きく二分される。パブリッククラウドとはインターネットを介して不特定多数のユーザを対象に利用されることを前提に構築･提供されるクラウドサービス、プライベートクラウドとは特定のユーザが利用することを前提に構築･提供されるクラウドサービスと整理されている。さらには両者の中間的な存在であり、同じ目的を持つ特定ユーザ群によって形成される「コミュニティ」に閉じて共同利用されるようなものをコミュニティクラウドと定義する考え方もある。

本節では、民間ベースの商用パブリッククラウドや、各府省等に閉じて利用される府省クラウドであるプライベートクラウドに加え､各府省で共同利用される政府共通プラットフォームのようなコミュニティクラウドも含めた分類とし､そこにオンプレミスと呼ばれる従来型のクラウドを用いない形態も含め、パブリッククラウド、プライベートクラウド、コミュニティクラウド、オンプレミスの４つについて、選択の考え方を整理する。

また、クラウドの形態は、前述の利用対象に加えて、提供されるサービスが、SaaS(Software as a Service)と呼ばれるアプリケーションレベルか、PaaS(Platform as a Service)と呼ばれるプラットフォーム(アプリケーションの動作環境)レベルか、IaaS(Infrastructure as a Service)と呼ばれるインフラ(ハードウェア及び iDC)レベルなのか、という観点での分類も重要となる。

これらの利用対象と提供サービスによって、クラウドを分類し、例示したものが「図 4.8-1 クラウドの分類と例」である。また、クラウドの利用については、複数のものを組み合わせて利用するハイブリッド(複数種類を組み合わせて利用)、マルチ(複数事業者のサービスを組み合わせて利用)等の選択肢もあり、適切な事前評価が必要となる。

	パブリッククラウド	コミュニティクラウド	プライベートクラウド	オンプレミス
SaaS	Webメール関連機能提供商用サービス CRM関連機能提供商用サービス等	政府共通プラットフォーム 自治体クラウド(自治体ASP)	省内クラウド（共通業務）	業務アプリケーション
PaaS	業務アプリケーション動作環境提供商用サービス	政府共通プラットフォーム 自治体クラウド(共同センタ)	省内クラウド	インフラ
IaaS	インフラ提供商用サービス	政府共通プラットフォーム 自治体クラウド(共同センタ)	省内クラウド	

図 4.8-1 クラウドの分類と例

一般論としてクラウドを利用することは、主としてスケールメリット、仮想化技術、オンデマンド利用等の観点からコスト削減が期待できる。例えばIaaSレベルにおいては仮想化技術によりマシンの利用効率が向上し、それに伴うコスト削減が期待できる。オンプレミスであれば、個々のシステムのピーク時負荷に合わせてサーバを構成するが、これは、ピーク時でない平常時においては、多くのリソースが有効に活用されていないということである。PaaS レベルにおいては IaaS での効果に加え、様々なソフトウェア製品や運用・保守のコストについてもコスト削減が期待できる。SaaS レベルにおいては、さらに業務パッケージの導入と同様に業務アプリケーションの開発保守についてのコスト削減が期待できる。もちろん、クラウドには、クラウド化に伴う様々なコスト増大要素も存在する。しかし多くの場合においては、それらを上回るコスト削減効果が期待される。

クラウド適用を検討する個々のシステムについては、オンプレミスも含めどのような形態が最適かを判断する必要があるが、その際に重要となるのが、コスト、迅速性、データ連携、サービスメニュー、法的な制約、セキュリティ上の制約、サービスレベル等となる。また、最適と想定されるクラウドサービスが、具体的に存在しない場合は、代替案の選択が必然となる。以下に各要素の各々について、その考え方を述べる。

- コスト

一般論としては、パブリッククラウドが最も低コストであり、コミュニティクラウド、プライベートクラウドと続き、オンプレミスが最も高コストと考えられる。その根拠としては、スケールメリットに加えて、総合的な効率性への期待と、商用パブリッククラウドの実際の低廉な料金体系という実績が存在する。特にパブリッククラウドの IaaS を使用する場合、通常時は通常負荷に合わせて最小限の構成のみを契約し、ピーク時間帯や繁忙期

にのみ構成を追加することも可能となること、また、短期的、一時的な利用においても、合理的な費用で利用できるという、オンデマンド利用の一面から、新たなコストメリットの発現も期待される。

コストの中心となる利用料金については、個々の事業者が決定、コントロールする事項なので、一般論とは異なるケースも多く想定される。特にコミュニティクラウドやプライベートクラウドが、クラウド構築組織の予算によって構築される場合、クラウド利用部門については、発生する実コストとは異なる考え方の課金が設定される可能性もあり、利用部門のコストが政策的に決定される可能性も想定される。その場合は、利用部門に閉じた最適解と全体最適解が異なる可能性も想定されるので、より高度な判断が求められる可能性がある。

また、利用料金に加えて、クラウド利用のための業務の見直し、前述のハイブリッドやマルチへの対応、移行・導入、追加的なセキュリティ対策等の付加的な費用も発生するため、これらも含めた総合的な評価が必要となる。

・ 迅速性

PaaS や IaaS 等のクラウドサービスで一般的に標榜されているオンデマンドとは、即時にサービスが利用可能となることである。これは、従来は業務システムごとにオーダーメイドで設計・構築していたインフラ環境を、あらかじめ標準化、メニュー化し、レディーメイドで提供することによって実現される。よって、PaaS や IaaS であれば、パブリッククラウド、コミュニティクラウド、プライベートクラウドにかかわらず、十分な迅速性を有することが期待される。しかしながら、コミュニティクラウド、プライベートクラウドについては、構築者によりオンデマンド性に十分な配慮がなされず、サービスが利用可能となるまでに、従来のオンプレミスと同等のプロセス、時間を要することも想定される。また、サービスメニューの洗練度の不足から、利用形態の検討に時間を要する可能性もある。それらに複雑な検討、調整を要する場合、クラウド利用者とクラウドサービス提供者の調整は複数組織間の調整となることから、オンプレミス以上に時間を要する可能性も存在する。

SaaS においては、クラウド利用のための業務の見直し、連携機能の検討も含まれるため、パブリッククラウド、コミュニティクラウド、プライベートクラウド、オンプレミスにおいて、一般論としての明確な優位・劣位は想定されず、ケース・バイ・ケースの評価になると考えられるが、単純で小規模な業務、特定機能に絞っての利用であれば、パブリッククラウドが有利になる可能性が期待される。

・ データ連携

政府共通プラットフォームのようなコミュニティクラウドに特に期待されるのが、データ連携機能である。これは、PaaS の機能の一環とも考えられるが、クラウドが提供する共通的な機能の利用によって、同じコミュニティクラウドを利用するシステム間で、高度なデータ連携がセキュアかつ低コストで実現可能となる仕組みである。

この効果が最も期待できるのは、コミュニティクラウドであり、例えば政府共通プラットフォームにおいては、府省をまたがったシステム間のデータ連携、府省共通システムと各府省固有システムとの連携、さらには政府共通プラットフォームを利用する同一府省のシステム間の連携まで期待できる。

次にこの効果が期待できるのが、プライベートクラウドとなる。しかし、その効果は府省内に閉じたシステム間の連携にとどまる。

パブリッククラウドとオンプレミスにおいては、データ連携には従来通りのアプローチが必要であり、特に追

加となる効果は期待されない。

・ サービスメニュー

既存システムをクラウド上に移設する場合は、IaaSかPaaSの選択となるが、クラウド利用のハードルが比較的低く、その効果も比較的低いのがIaaS、ハードルが比較的高く、その効果も比較的大きいのがPaaSと考えられる。既存システムをIaaSにのせるには、既存システムが必要とするOSやDBMS等がサービスメニューに用意されていれば、概ね可能だが、PaaSにのせるのは、それ以外の運用管理や処理方式の見直しに踏み込む必要があるためである。いずれにしても、既存システムをクラウドに移設する際に、既存システムに発生する改修作業は最小化されるべきと考えられるので、可能な限り改修が発生しないようなサービスメニューを選択する必要がある。

逆に、新規システムをクラウド上に構築する場合は、SaaSの活用から検討を開始し、IaaSよりもむしろPaaSを利用するように検討を行うべきである。そのためには、当初からクラウド利用を前提とした設計、調達仕様とする必要がある。オンプレミスを前提としていたり、クラウド利用の観点の欠如した設計、調達仕様では、クラウドの有効利用は難しい。

また、ハイブリッドやマルチについても、明確な利用イメージが固まっており、その効果が十分に期待できる場合は、積極的に取り組むべきと考えるが、インタフェース部分の設計や障害時対応、セキュリティ等も含めた責任分界については、十分に留意されたい。

・ 法的な制約

一般論としては、パブリッククラウドが最も法的な制約を受けやすく、コミュニティクラウド、プライベートクラウドと続き、オンプレミスは最も法的な制約への対応が容易と考えられる。しかしながら、実際は個々事業者に依存する領域であり、詳細は「4.8.2. 制度上の留意点」を参照されたい。

・ セキュリティ上の制約

一般論として、データ保管に関するセキュリティについては、そのサーバの設置場所、データの保管場所から、パブリッククラウドが最も課題が大きく、次がコミュニティクラウドとなり、プライベートクラウドが最もオンプレミスに近い状況となる。また、データやシステムを集中化させるという観点からも、パブリッククラウドが最も課題が大きく、コミュニティクラウド、プライベートクラウドと続き、オンプレミスが最後となる。

しかしながら、セキュリティ技術や運用については、大規模なクラウドの方が専門家の知見とコストを集中的に投入できる可能性が高い分、かえって優位であることも想定される。

実際は個々事業者に依存する領域であり、詳細は「4.10 セキュリティの考え方」、「6.12 セキュリティ」を参照されたい。

・ サービスレベル

一般的にクラウドサービスの利用に際しては、クラウド利用者からクラウド事業者のシステムや運用の状況が見えにくいため、障害等でダウンしてしまわないかという懸念に加え、当事者間の責任分界点が見えにくいという懸念も存在する。このため、パブリッククラウド、コミュニティクラウド、プライベートクラウドのいずれにおいてもサービス内容・範囲・品質等に関する保証基準の共通認識としてSLA(Service Level Agreement)が、クラウドサービス提供者から提示されるべきである。

サービスレベル自体については、個々の提供者に依存するものであり、パブリッククラウド、コミュニティクラウド、プライベートクラウド、オンプレミスについて、一般的な相違はないと考えられる。詳細については「4.8.3 事業者・サービス選択時の留意点」を参照されたい。

4.8.2.制度上の留意点

クラウドの利用に際しては、制度面においても注意が必要となる。以下に「データの保存場所」、「個人情報保護法との関連」、「医療情報システムの安全管理に関するガイドライン」、「ASP・SaaSの安全・信頼性に係る情報開示指針」、「著作権法上の問題」、「e 文書法との関係」、「外国為替及び外国貿易法」の各々の観点より留意点を記述する。

・データの保存場所に関して

クラウドを利用するときに問題となるのが、データがどこに存在するのかがわからないということである。データは、海外の一つの国に存在するのみならず、国を移転しながら保管されることもありうる。データの保護に関する法律は、データが存在する国の準拠法に基づき行われるため、データが存在する国の法律に注意を向ける必要がある。ただし、クラウド事業者によっては、データがどこに存在するのかを示していない場合がある。

例えば、米国では、Electronic Communications Privacy Act (ECPA:電気通信プライバシー法)に基づき、令状なしで行う捜査当局に対する通信の開示を禁止しているが、PATRIOT Act(愛国者法)では、捜査当局の権限が強化されており、データセンターから捜査当局が必要と認識するデータを持ち去られる可能性がある。また、一部ではインターネット検閲が行われている国も存在する国際状況でもあり、クラウドを利用する際には、そのデータの保管場所を明確に認識する必要がある。

・個人情報保護法との関連

日本では、個人情報保護法 22 条により、「個人情報取り扱い事業者は、個人データの取り扱いの全部又は一部を委託する場合は、その取り扱いを委託された個人データの安全管理が図られるよう、委託を受けたものに対する必要かつ適切な監督を行わなければならない。」と規定されている。また、第 23 条において、一部の例外ケースを除き、本人の同意を得ずに、個人データを第三者に提供することは禁じられており、第 16 条においては、収集時に特定された利用目的以外の目的で、本人の同意を得ずに、個人情報を取り扱うことも禁じられている。一方で、個人情報の保管場所に関する制約はなく、委託先の監督など「個人情報保護法」で規定される事項を遵守する限りにおいて、国外も含め第三者の提供するサーバ上に個人情報を保管することは可能である。

他方、EU のデータ保護指令では、EU 内の住民の個人情報に関して十分なデータ保護レベルを確保していない第三国へのデータの移動を禁じている。EU のデータ保護指令が要求する十分な保護水準を確保していると認められている国･地域は、スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島、フェロー諸島、イスラエルの８つである(平成 22 年 11 月現在)。米国の場合は、セーフハーバー協定により､登録を行えば､個人情報保護上問題ないと認識される。EU においては、日本は個人情報保護が適切に行われていないと認識される場合がある。

・医療情報システムの安全管理に関するガイドライン第 4.1 版(平成 22 年 2 月）

医療情報システムの SaaS に関しては、｢ASP/SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン｣をもとにして､｢所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP･SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ･ストレージ等は国内法の適用が及ぶ場所に設置すること。」とあり、ガイドライン遵守の観点からは、事実上、海外のデータセンターを利用することは難しい。

・ASP･SaaS の安全･信頼性に係る情報開示指針

クラウドサービス事業者側のプライバシー保護、監査可能性等については、平成 20 年 4 月から、ASP･SaaS 事業者の安全性･信頼性に関する情報開示の仕組みとして､｢ASP･SaaS の安全･信頼性に係る情報開示指針」に基づく認定制度が開始されている。ただし、事業を行うのに、この認定が必須ではなく、この制度が海外のベンダーも含めて認知度を高め、クラウド事業者が認定をとらないと事業が成立しない状況にならないと有効に機能しない。普及状況にもよるが、利用者側からは、この認定を受けているかどうかが選択の一つの基準とすることができる。

・著作権法上の問題

平成 22 年 1 月 1 日から改正「著作権法」が施行され、情報検索サービスを実施するための複製等に係る権利制限や情報解析のための複製等に係る権利制限等、一定の見直しがなされてきた。

しかし、諸外国で既に類似の実施例があるものの、我が国の「著作権法」ではなお違法となる可能性があるとして、事業者によって懸念が示されているサービスが存在している。例えば、著作物をストレージサービスで預かる行為や､著作物の内容をクラウド上で解析して付加価値を提供するサービス等に関してクラウド事業者の間接侵害を問われる可能性が懸念されている。また、レコメンデーションを行うサービスやサムネイル表示などマルチメディア著作物の引用などについても違法となる可能性が懸念されている。

・e 文書法との関係

平成 17 年 4 月から施行された「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(以下、e-文書法)」などにより、約 250 種類の法律を対象として、各種書面に代えて電

磁的記録の保存を認めることとした。しかしながら、「e-文書法」の目的は、あくまで紙情報の電子化であり、その記録を外部のサーバへ保管することに関しては、必ずしも考慮されていない。その結果、個別の法令によっては、データの外部保存に関して一部制約が残っている。

例えば、「割賦販売法施行規則」においては、帳簿を主たる営業所に備えることが、また、「法人税法施行規則」においては、帳簿を納税地に保存することなどが規定されているため、一般的なクラウドサービスを利用するのに制限がある。

・外国為替及び外国貿易法

「外国為替及び外国貿易法(以下、外為法)」では、国際的な平和及び安全の維持を妨げることがないように、特定の技術を特定の外国において提供する際や特定の外国人・外国企業に提供する際には、経済産業大臣の許可が必要と定めており、第 25 条第 3 項では「特定国において受信されることを目的として行う電気通信による特定技術を内容とする情報の送信」も許可の対象として規定している。従って、日本国内から海外の外部サーバに情報を送信する際や、当初から外国の利用者に情報を提供することを目的に自らの海外設置サーバに情報を送信する際、国内サーバのリソースを演算処理等のために提供してその結果を送信する際等も、許可の対象となる場合がある。

この特定技術とは、核兵器等の大量破壊兵器や通常兵器に関連した技術を指しており、例えばこの技術の中には暗号技術などの汎用的な技術も多く含まれるため、これらの情報を取り扱う際には留意が必要である。

4.8.3.事業者・サービス選択時の留意点

クラウドの利用に際しては、事業者・サービス選択においても、注意が必要である。以下に「サーバの設置拠点及びデータ格納地域」、「マルチテナントの管理方法」、「情報セキュリティ対策」、「経営の継続性」、「サービス機能」、「SLA」、「サービスの継続性」、「サービスコスト」、「サービス事業者切り替え時のシステム環境の継続性」、「サービス終了時のデータ削除の証明」の各々の観点より留意点を記述する。

・サーバの設置拠点及びデータ格納地域に関して

クラウド事業者は、複数拠点にサーバやストレージを配置し、可用性を満足するために、それらの複数のサイトを複合的に利用することでクラウドサービスを提供する場合がある。この場合、クラウド事業者は、必ずしも拠点を明示しているとは限らないことに留意が必要である。ただし、最近では特に企業ユーザの要望により、どの範囲にデータを保持するかを明確にするクラウドベンダーもあり、実際の選択時には留意する必要がある。

・マルチテナントの管理方法

クラウドサービスでは、いわゆるプライベートクラウドを除き、複数の企業や事業体が同一の環境を利用する。このため、いわゆるマルチテナント間のセキュリティに関して、もしくは可用性に関し

て十分な対策がとられていることが必要になる。また、より機密性を要求される場合には、IPsec VPN等の活用により、プライベートクラウド並のセキュアな環境が必要なこともあり、クラウド事業者のセキュリティ面での提供サービスにも留意する必要がある。

・情報セキュリティ対策

クラウド事業者が、ISMS制度(JIS Q 27001：2006、ISO/IEC 27001：2005)や経済産業省のプライバシーマーク制度に対してどのような対応をとっているのか。また、内部統制の監査の観点からは、利用する部外者が監査を受け入れる体制があるのか。できない場合には、「SAS70(Statement on Auditing Standards No.70、米国監査基準書70号)」、もしくは、「日本公認会計士協会の監査基準委員会報告書第18号「委託業務に係る統制リスクの評価」(通称：18号監査)」の報告書を提供しているのか。特に、運用が適正に行われているかどうかであるので、SAS70の場合はTypeⅡ(運用状況の報告)等も重要な評価要素となる。

・経営の継続性

サービス基盤を提供業者に依存するため、そのサービスが継続的に提供されるか否かが重要である。このため、サービス提供業者の経営基盤がしっかりしているのかに関しても留意する必要がある。特に、海外のサービスベンダーに関しては、実態が明らかでない場合もあるため、十分確認の上サービスを利用すべきである。

・サービス機能は満足しているか

必要なサービスを発注者側の要件により決めることはできず、クラウドサービス事業者により提供されているサービスを利用することが基本となる。このため、パッケージと同様に、必要な要件と提供されているサービス機能のFIT/GAP分析を行い、GAPに関しての回避策を考慮の上、サービスを選択する必要があることに留意すべきである。

・SLAが顧客側の要件を満たしているか

クラウド事業者は、広くサービスの提供を行っているため、個別のSLAは結ばないことが多い。また、主要なパブリッククラウド事業者から提示されているSLAは稼動率のみであり、パフォーマンスやバックアップ、障害リカバリ、セキュリティレベルなどについては触れられていないのが現状である。このため、クラウド事業者の提示しているサービスレベルを確認の上、そのサービスレベルで問題がないかを検討するとともに、利用者側の必要とするサービスレベルが不明な場合は、クラウド事業者にサービスレベルの不明点に関して極力確認の上、契約することにも留意する必要がある。
また、通常はサービスレベルの高いものが高く評価されるが、サービスレベルとコストはトレードオフであり、高いサービスレベルは高コストとなることが多い。いずれにおいても、システムに対するニーズや利用状況を把握した上でコスト等を考慮し、提示されたサービスレベルが妥当かどうか判

断する必要がある。

・サービスの継続性

提供されているサービスは、サービス提供業者により、改善のためにバージョンアップが行われることがある。この場合、サービスの継続性の面で問題がないかどうかについて確認する必要がある。サービス提供業者に対して、バージョンアップ情報の早期の提供を求め、サービスが継続的に利用可能となるよう、留意する必要がある。

・サービスコスト

クラウドサービスに関しては、サービスを利用した分だけ費用を支払う契約となることが多い。コストに関しては、経済環境や競合環境などにより、変更することが考えられる。変更した場合の対応に関しても、サービス利用開始時点から留意する必要がある。また、利用する期間を考慮の上、本当にクラウドサービスを活用した方が安くなるのかどうかも、ライフサイクルを通してのトータルコストの観点から精査することに留意する必要がある。

・サービス事業者切り替え時のシステム環境の継続性

サービス事業者を切り替えるに当たって、利用している開発環境、開発ツール、実行環境、データ等を次の業者に移行できるかどうかに関して、あらかじめ検討する必要がある。特に、SaaS の場合に、選定業者独自の実行環境を提供している場合が多いため、データをその項目としてダウンロードできるかどうかを確認する必要がある。

・サービス終了時のデータ削除の証明

サービスの契約解除時には、既存のデータを保存の上、単なるデータ削除ではなく、データの復元ができない状態に完全に削除･消去を行う必要がある。特に、機密性の高い情報を扱った場合には消去が完全に行われた証明書の提出を要求することも必要となる。

4.8.4.調達･契約時の留意点

クラウドの利用に際しては、調達･契約においても注意が必要である。以下に「クリックラップ契約」、「分離調達(調達基準)との関係」、「調達先の固定化の回避」、「インターオペラビリティの確保」の各々の観点より留意点を記述する。

・クリックラップ契約(シュリンクラップ契約)

ソフトウェアパッケージのシュリンクラップ契約と同じように、クリックラップ契約(もしくは、クリックオン契約)である場合がある。この場合は、同意書をクリックした時点で、契約が結ばれたことになるので留意が必要である。なお、こうした契約の有効性については、US においてシュリン

クラップ契約が有効と認められた判例があるが、クリックラップ契約は有効と認められた判例はない。日本ではどのように判断されるか不透明であるが、クラウドの利用に際して、契約形態については十分確認する必要がある。

・分離調達(調達基準)との関係

アプリケーションとシステム基盤に関しては、分離調達が推奨されているが、SaaS 型のクラウドサービスの場合は、そのサービスを利用する形態となるため、システム基盤を選択する余地がない。また、アプリケーションを PaaS 上で作成する場合も、PaaS 事業者による依存関係が生じてしまうため、PaaS を決めた上で、アプリケーションを見積もる必要が出てくる。IaaS を開発基盤として検討対象とする場合は、IaaS の開発基盤上でアプリケーションを構築することになり IaaS と不可分の関係となるため、IaaS を利用するのかどうかを、アプリケーション調達前に判断する必要が出てくる。

また、IaaS/PaaS 上で、SaaS 形式でサービス提供するような複数事業者が関連する可能性があり、この場合には、トラブル発生時に問題を早期解決するため、IaaS/PaaS 事業者と SaaS 事業者の責任範囲を明確化しておくことが必要である。

・調達先の固定化の回避

政府調達としてサービスの提供を受ける場合は、期間を提示の上、契約を行うことになる。契約更新の場合、調達のオープン化のために競争入札を行う必要があり、そのサービスを他のサービス提供事業者等に切り替える可能性が生じる。その際、機能の継続性の観点から、別なサービス事業者に円滑にサービス及びデータの引き継ぎができるかどうかが重要である。特に PaaS の場合には、その環境で開発が行われるために、別な環境では開発したアプリケーションが動作しないことが想定されるため、調達に際しては十分留意が必要である。SaaS の場合は、データの移行がスムーズに行われるかどうかがポイントになる。

・インターオペラビリティの確保

他のシステムとの連携を考慮する必要がある場合には、そのサービスが他のシステムとの連携が可能かどうかの検討を十分に行う必要がある。また、連携した場合に、サービスレベルやセキュリティレベル上問題がないかどうかについても十分に確認を行うことに留意が必要である。

4.9.クラウドを構築する立場からの考え方

本節では、クラウドを構築する観点から考慮すべき点を記述する。クラウドを構築する立場には、調達者としてクラウド構築にかかわる立場と、応札者として実際にクラウドを構築する立場の２通りがある。最終的に利用者へクラウドサービスを提供する立場は同じであるが、クラウドを調達・構築する際には、立場の異なる双方の観点が必要となる。

各府省で構築するクラウドは、主にプライベートクラウドに分類されるものである。以下本節ではプライベートクラウドを前提として考え方を記述するが、複数の府省で共同利用するコミュニティクラウドや、複数のクラウドからなるハイブリッドクラウドについても考慮が必要である。

4.9.1.クラウドの構成要素

クラウドには様々な構成要素があり、提供するサービスがSaaSか、PaaSか、IaaSかによって、構築に用いる構成要素の種類や実装が異なる。一般的なクラウドでは、ハードウェアやソフトウェアなどの IT リソースが、利用者の必要に応じて(すなわちオンデマンドで)提供されるように「リソースプール」という形態で用意されている。これらのリソースは、「ネットワーク基盤」と「運用管理基盤」とによって、ネットワークを通じた情報処理サービスとして利用者へ提供される。SaaS や PaaS では、業務サービスを提供するアプリケーションソフトウェアや、アプリケーションを実行させるための動作環境やデータベースなどのソフトウェア資源を、あらかじめ何種類用意し、どの程度まで実装・プールしておくか、といった構成要素ごとの詳細な検討が必要となる。

・ IT リソース

クラウドのハードウェアリソースとしての基本的な構成要素は、サーバとストレージである。クラウドでは一般に物理サーバやストレージには仮想化技術が適用され、OS を搭載した仮想サーバが仮想化されたストレージと共に情報処理を実行する。物理的なストレージは、物理サーバに内蔵されたディスク装置の場合と、物理サーバとは別のストレージ装置の場合とがある。

・ ネットワーク基盤

ネットワーク基盤は、主にクラウドシステム内の LAN 機能と、外部ネットワークとの接続インタフェース機能を提供する。サーバーストレージ間の高速大容量データ転送を担う NAS/SAN も、ネットワーク基盤の構成要素の一つである。ネットワークにも仮想化技術が適用され、VLAN などの仮想化されたネットワークが提供される。なお、負荷分散や SSL アクセラレーションのように、情報処理サービスと共に用いられるネットワークの特殊な機能は、オンデマンドで提供できる IT リソースとしてリソースプールに含める場合もある。

・ 運用管理基盤

運用管理基盤は、通常システムの場合と同様の監視・制御機能と、クラウドシステムに特化した運用管理機能の双方を提供する。特に、クラウドでは仮想化・自動化技術の適用により、ダイナミックなプロビジョニングやデプロイメントを実行・管理する機能が必要になる。また、サービス利用者の ID 管理やセキュリティ管理、サービスメニューや管理ポータルなどのユーザインタフェースの提供や SLA 管理も運用管理基盤の役割である。

通常のシステムにクラウド・リソースを適用した一例を図 4.9-1 に示す。この適用例は、図 4.2-1 のネットワーク物理構成モデルにおいて、一部のサーバをクラウドで提供した場合の構成例である。図 4.9-1 において、角丸長方形で囲んだ部分がクラウド・リソースによるサーバ群を示す。複数のネットワークセグメントに分散しているサーバ群の各々を対象として、クラウドの適用が可能である。なお、本図は、各構成要素間のネットワーク接続関係を示した図であり、ネットワーク基盤の詳細や運用管理基盤については図示を省略している。

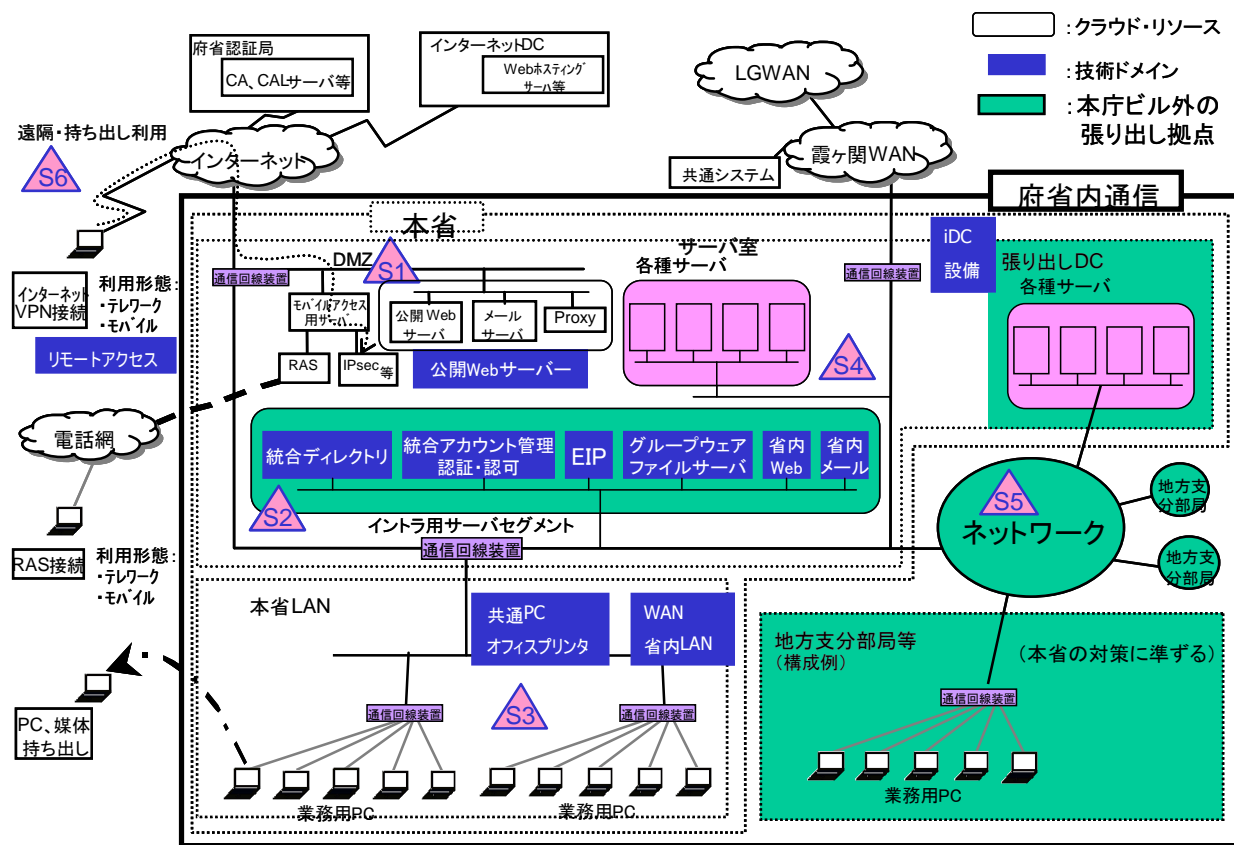



図 4.9-1 クラウド・リソースの適用例

4.9.2.サービスメニューの考え方

クラウドのサービスメニューとは、クラウドサービスの提供者が、利用者に対して標準的に提供するサービスの内容を標準化、一覧化したものである。これによって、迅速で安定したサービス提供が可能になる。サービスメニューには、サービスメニューごとの選択肢、サービスメニュー全体に共通する選択肢などがある場合もある。

サービスの内容は、ある程度の幅で選択肢を持たせるものの、基本的には限られたパターンに標準化されたものにし、サービスメニューに明記することが望ましい。これによって、サービスの均質化を図ることができ、リソース利用の効率化、サービス品質の向上などの効果を期待できる。また、サービス提供プロセスの一部、あるいは全体を自動化するなどして、サービス提供を迅速化することができる。

サービスの提供単価は、サービスメニューとその選択肢によって、個別に設定することもある。利用者の選択に応じて価格を増減することで、一定の利用パターンに利用者を誘導したり、共有リソースの合理的な利用を促進したり、する効果が期待できる。

サービスメニューにないサービスを、例外的に提供する場合も考えられる。この場合は、サービスメニュー外でのサービス提供となるため、要件の決定、価格の見積もり、後述する SLA の合意に時間がかかるほか、場合によっては追加調達や開発などのために、サービス提供可能となるまでに時間がかかったり、投資回収の観点で不利になったりするので、全体最適の観点からは必ずしも好ましい結果とならない場合がある。

4.9.3.SLA の考え方

クラウドの SLA とは、クラウドサービスの提供者が、利用者に対して提供する標準化されたサービスの品質について提示し、迅速なサービス提供を可能にするものである。前述のサービスメニューにおけるメニューや選択肢の指定を通じて、提供する SLA を選べる場合もある。

SLA に対する要求を決定するビジネス上の理由や、実現する SLA を左右する技術・運用面での要素については、クラウドにおいても本質的な違いはない。しかし、指定された SLA の要件に基づいて個別に設計するシステムとは異なり、クラウドではサービス提供者側が、SLA の要件を想定してサービスを設計している点が大きく異なる。このため、クラウドにおける SLA とは、サービス提供者側が、選択肢を含む内容を、サービスメニューを通じて提示し、サービス利用者がその中から選択する、という形で合意形成されるものとなる。

サービスメニューにない SLA 要件を実現するサービスを、例外的に提供する場合もある。この場合は、サービスメニュー外でのサービス提供となるため、要件の決定、価格の見積もり、場合によっては追加調達や開発などのために、サービス提供可能となるまでに時間がかかったり、投資回収の観点で不利になったりするので、全体最適の観点からは必ずしも好ましい結果とならない場合がある。

4.9.4.ユースケースと要件

クラウドサービスの要件は、クラウドサービス構築、利用にかかわる登場人物(プレーヤー)を特定し、それぞれの要件を洗い出すことになる。以下に登場人物を示す。要件はどの立場に立っているのか明らかにする必要がある。

・プロバイダ:SaaS、PaaS、IaaS 環境を提供する。

サービスとリソースの双方を視野に入れたセキュリティの配慮　、クラウドが提供するリソースの保全性、完全性、信頼性、クラウドが提供する効果的なリソースの操作、データ・サイズ、タスク数やユーザ数へのス

ケーラビリティ等に対する考慮

・コンシューマ：プロバイダが提供するサービス環境上に実際のサービスを構築する。
短期稼動、従量課金等に対する考慮

・エンドユーザ：クラウド上に構築されたカスタマサービスを利用する。
サービスの種類と機能、サービスの可用性と信頼性、クラウド上のデータとリクエストの完全性、プライバシー等に対する配慮

・イネーブラ(ベンダー)：プロバイダやコンシューマに物品や役務を提供する。

・オペレータ：クラウド環境を運用する。

4.9.5.クラウド構築時の留意点

クラウド環境を構築する際に考えておかねばならない留意点を挙げる。

- SaaS/PaaS/IaaS のサービスごとに、最適な仮想化機構、適切な仮想環境管理基盤などを選択してシステム設計を行い、運用設計を行う必要がある。
- 対象としているサービス利用者に対して、適切なサービスメニューを用意し、サービスメニュー(管理ポータル、監視/統計システムなど)を実際に提供するための運用管理基盤を構築する必要がある。
- 各テナントのリソース利用状況に気を配る必要がある。
- 需要に応じスケールイン・スケールアウト可能な構成とするべきである。
- 単一故障点をなくすべく検討しなければならない。
- 監視、バックアップ、ジョブ実行、ログ、認証などの機能は、可能な限りクラウドシステム全体で共有できるモデルがよい。
- 複数のクラウド環境を組み合わせたハイブリッドクラウドを構築する場合は認証/ユーザ管理/課金管理等の検討が必要である。
- 責任分界点、SLA を利用者に提示することが必要となる。
- サービス利用者に対する SLA を適切に定め、それを実現するための監視/制御システムを構築する必要がある。
- 将来のクラウドサービス環境の移行を成功裏にかつスムーズに進めるために移行完了基準を明確にしておく必要がある。
- 提供する環境や VM イメージのセキュリティチェックに留意するべきである。
- 複数のサービス利用者がリソースプールを共用する場合の性能設計/増設計画/セキュリティ設計を適切に行う必要がある。
- 外部からの制約(EU データ保護指令や米国愛国者法のような国内外の法規制、 地震や気象条件のような地理的な状況、電力コストとキャパシティ、送電網の余剰率や信頼性、ネットワークの帯域幅など)の考慮が必要な場合があることを念頭に置かねばならない。

4.10.セキュリティの考え方

情報セキュリティは、情報システムを活用し、「安全」「安心」を社会システムや業務に提供するものであり、単なる情報システム上のセキュリティ機能だけを意味するものではない。情報セキュリティは、ISMS(Information Security Management System)を構築し、情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)を確保することである。

情報システムは、コンピュータウイルス、不正侵入、サービス妨害等の外部からの「脅威」や、セキュリティ機能の欠如、不適切なソフトウェアの運用管理等の内在する「脅威」にさらされている。また、これらの脅威により問題が発生する可能性を「脆弱性」と呼び、この脆弱性は情報システムから完全には排除できない。この完全には排除できない情報システムの脆弱性に対して脅威が作用し、事故、障害等の「インシデント」が発生し、情報システム、社会システム、業務に対して好ましくない「影響」を与える。この一連がセキュリティが維持できなかった場合の連鎖である。

このような連鎖が起こらないようにセキュリティを確保するためには、3つの対処の観点から対応することが必要であると考えられる。

- セキュリティに関する技術的対処

  導入する情報システムに対して、セキュリティ機能を実装すること。各技術ドメインのセキュリティ条件や非機能要件のセキュリティ等が該当する。

- セキュリティに関する組織的対処

  セキュリティを確保し、情報システムを運用する組織体制を整備すること。

- セキュリティに関する運用的対処

  整備されたセキュリティに関する組織体制を活用し、情報システムをセキュリティに関して適切に運用すること。役務調達共通もしくは役務調達分類に応じたセキュリティに関する留意点等が該当する。

また、一連の連鎖を起こさせないためのセキュリティ対策としては、以下の2通りのセキュリティ対策があることにも留意する必要がある。

- 脅威や脆弱性を排除し、インシデントを起こさせないセキュリティ対策
- インシデントが起きる可能性はあるが、インシデントが最終的な影響を与えないセキュリティ対策

セキュリティを強化することは、コストと運用性を考慮しなければ、際限なく行うことができる。セキュリティをどこまで強化するかは、以下の 2 点と対策を実施する際のコストと運用性のバランスを考慮し、決定するべきである。

- 「脅威」が「脆弱性」に作用し、「インシデント」を起こす可能性
- 「インシデント」の結果として起きる「影響」の大きさ

4.10.1.情報セキュリティに係る脅威と問題の変質

ここ数年の情報システムや通信ネットワークの動向を踏まえると以下のような情報セキュリティに係る脅威と問題が変質してきており、留意する必要がある。

- 情報システムや通信ネットワークに対する攻撃の多様化・高度化・複雑化

情報システムや通信ネットワークに対する攻撃はインターネットの黎明期から存在するが、ここ数年で攻撃の様相が大きく変化してきている。かつてのサイバー攻撃は、政府系や大手企業の Web サイトの改ざんによる自己の技術レベル誇示や政治的プロパガンダ、単なる愉快犯的な動機による組織の内部ネットワークへの侵入などが中心であり、攻撃の構造が比較的シンプルなものが多かった。近年になると、攻撃の目的が情報の詐取と詐取した情報を利用した金銭の奪取に変化し、攻撃が組織化する。具体的には、以下のような事例が見られる。(図 4.10-1)

- ✓ 攻撃目的に応じて、多段的な攻撃手法を自在に更新することによって攻撃成功の確率を高める攻撃
- ✓ アンチウイルスソフトによるパターンマッチングを用いたウイルス検出の精度を低下させるためにウイルス亜種による攻撃
- ✓ 被害が発覚しにくく、発覚しても影響が複雑で分析が容易でない、未公表の脆弱性を悪用するゼロデイ攻撃やターゲットを狙い撃ちする標的型攻撃

これまでは、共通の被害体験を組織の内外において共有し、問題対処に取り組んできた。しかし、上記の攻撃は、被害を共有化し、共有することが困難になってきており、効果のある対処をとることが難しい状況になってきており、単一の対策だけでは、対応しきれなくなってきている。

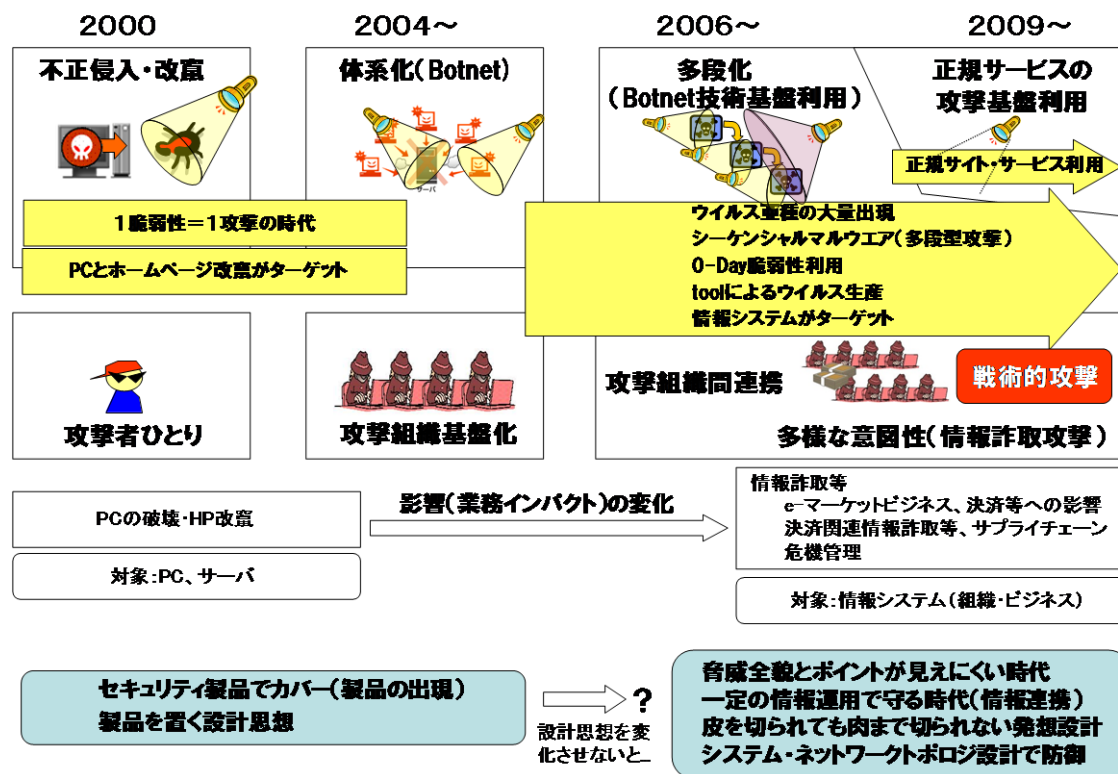



図 4.10-1 昔と今のサイバー攻撃の変化

- 組織への影響の意味と責任分界点の曖昧化

現在、情報システムが、ビジネスインフラとして不可欠な役割を担っており、ビジネスプロセスの様々な局面に浸透し、関係者も幅広く多様化・複雑化している。こうした状況では、仮にトラブルが発生した場合、責任の所在が曖昧になる可能性があり、トラブル発生時にどのような枠組みで対処するべきか明確ではない。
このため、問題解決には新たな対応が必要になってきている。

- セキュリティの意味の多様化

現在、情報システムが、単なるテクノロジを意味するのではないのと同様に、情報セキュリティ分野も、多くの社会システムやビジネスプロセスと関連するようになってきた。また、情報セキュリティの意味は、関連する社会システムやビジネスプロセスの立場によって異なる理解をされるようになってきて、意味の多様化が進んできている。このため、情報セキュリティの位置づけが、各立場のその責任や目的に応じて多岐にわたると同時に多様化が進んできている。(図 4.10-2) 情報セキュリティを議論する場合には、情報の受け渡しプロセスを整理し、どのような立場での情報セキュリティを議論しているかを明確にする必要がある。

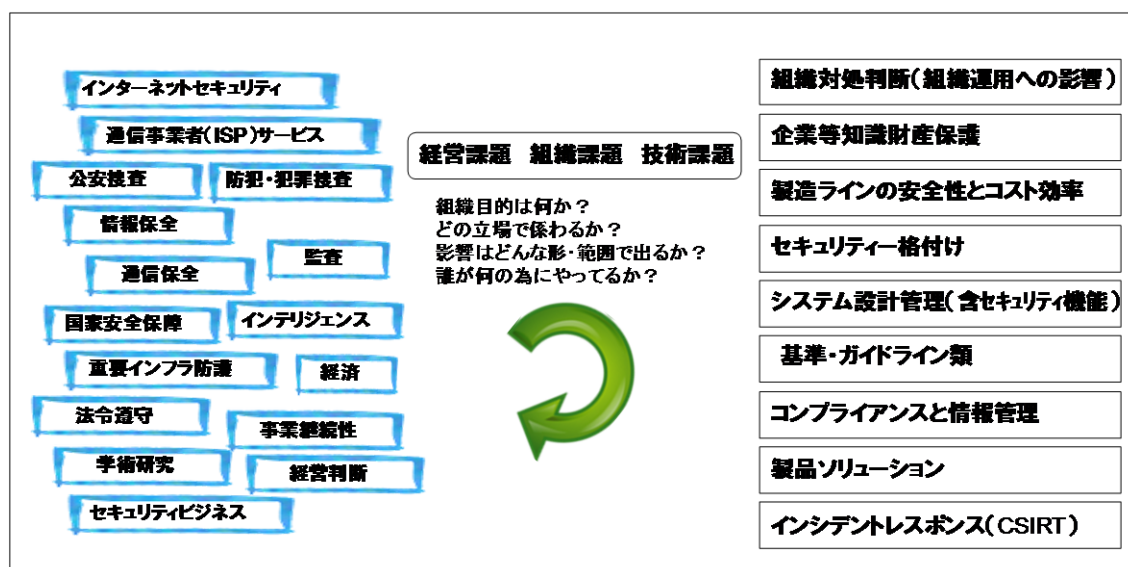



図 4.10-2 情報セキュリティ関連各分野

これらの情報セキュリティに係る脅威と問題の変質に着目し、サイバー攻撃防御(CND:Computer Network Defense)分野が注目されるようになってきている。

4.10.2.役務調達分類におけるセキュリティの位置づけ

役務調達に関しては、役務調達分類に応じてセキュリティを検討する必要がある。各役務調達分類のフェーズにおけるセキュリティに関して留意すべき点のポイントは、以下の通りである。

- 企画フェーズ

脅威、脆弱性、影響の大きさを考慮し、リスクの大きさを認識し、必要な対策のレベルを整理する。

- 要件定義フェーズ

企画フェーズで認識したリスクの大きさ、必要な対策のレベルに応じたセキュリティの要件定義を行う。

- 開発フェーズ

要件定義フェーズで、要件定義したセキュリティ対策を具体化し、運用・保守に必要なセキュリティ要件を整理する。

- 運用・保守フェーズ

開発フェーズで定義した運用・保守に必要なセキュリティ対策を実施する。また、経年による新たな脅威、新たな脆弱性、影響の変化に留意する。

4.10.3.情報セキュリティを企画・設計段階から確保するための方策(SBD)の概要

セキュリティ対策を行うにあたっては、上流の取り組みが下流に対して影響を与えることに留意し、前述の役務調達の全工程において、セキュリティポリシーの一貫性やトレーサビリティ確保、作業工程の手戻り回避などのためには、より上流での取り組みが期待される。

調達にあたっては、セキュリティ要件を意識して調達仕様に組み込まなければ、調達側と供給側の双方に不利益が発生する可能性がある。

具体的には、

① 情報システム調達における発注仕様書の不明瞭さ(や不公平さ)、調達から運用保守等の各段階における発注側と受注側の合意形成の困難さから、作業の手戻りや機材追加が発生するなどにより、追加コスト等の金銭的不利益が発生する可能性。

② 適切なセキュリティ要件を仕様書上に明確化していないことにより過剰あるいは不足が生じ、必要に応じた適切なセキュリティ対策が行われない不利益が発生する可能性。

といったものである。

こうした課題に対して、企画フェーズから、情報システムの調達側と供給側双方における不利益の発生を軽減し、適切なセキュリティ対策を確実に実装する必要がある。そのために、本技術参照モデルのほか、内閣官房情報セキュリティセンターにおいては、情報セキュリティ政策会議の要請を受け、「情報セキュリティを企画・設計段階から確保するための方策(SBD:Security By Design)に係る検討会(以下、「SBD 検討会」という。)」にて検討を行い、「情報システムに係る政府機関におけるセキュリティ要件策定マニュアル」を平成22 年度末に策定している。

当マニュアルは、政府機関において「新規構築」及び「更改」を行う情報システムの調達全般を対象とし、特に情報システムの調達を担当する行政事務従事者が当マニュアルを活用してセキュリティ要件を自ら責任を持って策定し、調達仕様書に記載できることを期待している。また、情報システムを供給する事業者においても、当マニュアルを参照することによって、調達仕様書に記載されたセキュリティ要件の理解を助ける情報(策定過程に関する情報等)を得ることが期待できる。

セキュリティ要件の導出にあたっては、情報システムにおける情報保護のための対策及びセキュリティ侵害への対策を踏まえ、重要かつ効果的な要件を優先的かつ確実に調達仕様書に記載することで、必要に応じた適切なセキュリティ対策の確保を期待している。

4.10.4.リスク要件リファレンスモデル(RM)の概要

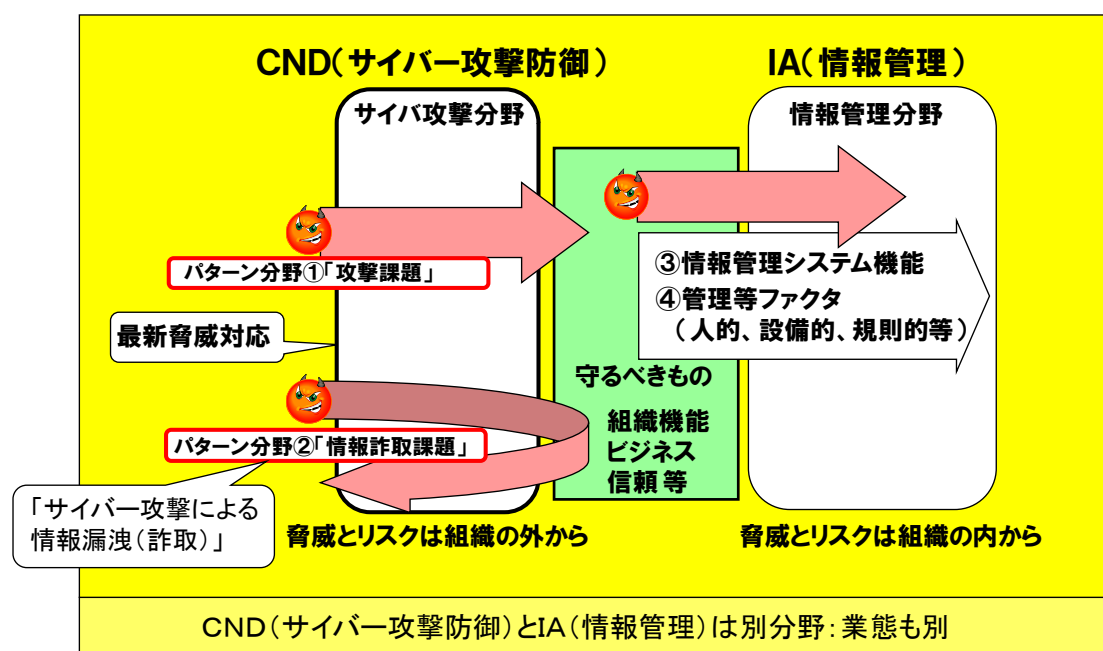
4.10.4.1.リスク要件リファレンスモデル(RM)の対象とするセキュリティ分野

情報システムのセキュリティ対策を、以下のように IA と CND に分類する。(図 4.10-3)

- ✓ IA(Information Assurance)：情報やデータの使用、処理、蓄積、伝送にかかるリスク及びそれらを目的として使用されるシステムやプロセスにかかるリスクを管理するための遵守行為のこと。本書においては、既存の指針(ガイドライン)や標準に従って情報管理を行うことにより情報の漏えいや改ざんを防止する施策のこと。
- ✓ CND(Computer Network Defense)：不正行為に対する防護、監視、分析、検知、そして対応(レスポンス)のためにとるべきアクションのこと。本書においては、外部からのサイバー攻撃に対して通信ネットワーク及び情報システムを防御してシステムの稼動を維持するとともに、情報の詐取を防止するための対応活動のこと。

IA 分野では、政府機関統一基準の整備により、内部統制システムを中心に体系的な整備が図られてきている。また、導入後の内部統制システムの運用においても、PDCA サイクルの実施が必要となっており、一定レベル以上での情報管理が求められている。一方、CND 分野は、ファイアウォールの導入、セキュアな通信プロトコルの導入、ウイルスチェックの導入などこれまでは個別対応に終始して来ている。これは、CND が対応するサイバー攻撃が多様であり、また攻撃手法の「進歩」のスピードが速いため、情報システムのセキュリティ担当部署では、変化し、進化するサイバー攻撃への個別対応に追われていることが理由の一つである。

情報セキュリティに係る脅威と問題の変質している近年においては、CND 分野においては、より一層体系的なアプローチが求められる。このためには、情報システムの調達時にセキュリティ対策を組み込む作業が初期段階(企画や要件定義のフェーズ)から組み込まれていることが重要である。

図 4.10-3 RM の対象分野

このような状況におけるサイバー攻撃防御（CND）分野の有効対策を考えるためには、リスク要件リファレンスモデル（RM）に基づく「現状脅威の正確な認識（脅威と影響の再定義）に基づく対策設計」を行う必要がある。

4.10.4.2.リスク要件リファレンスモデル(RM)の概念

「リスク要件リファレンスモデル（RM）」とは、高度化した CND 分野における現状脅威と組織への影響問題点の共通認識に基づくシステム設計対策の要否判断と実効性の確認された対策設計を可能とするアプローチ手法である。

従来対策としての「管理策」では、通常一意に設計対処が求められているが、現状のサイバー攻撃への対応に対する対策理由･効果の確認が課題となる一方、対策コストの増加傾向が発生する。

これに対し、RM では対策理由と効果を明確にしつつ、影響分析に基づく必要部分に重点的なシステム設計対策を行うアプローチとなっている。

また、近年、新たなサイバー攻撃スタイルが出現してから、従来のセキュリティ製品を置くシステム設計思想のみでは、対策効果が低下している。これに対応するため RM では、攻撃の実像と業務への影響を正確に把握した上で、必要性と効果を確認するための新しいシステムデザイン設計思想を取り入れた。（図 4. 10-4）

RM の分析アプローチを以下に示す。

① 現状のサイバー脅威の実像を具体的に分析整理した「攻撃パターン」を脅威モデルとして定義し、具体的な攻撃シナリオを整理。

② システムの特性ごとのシステムひな形として、情報システム設計モデルを設計。

③ 情報システム設計モデル上に攻撃パターンシナリオを攻撃トレース（机上模擬攻撃）することにより、影響と設計対策効果を分析。

④　攻撃トレース(机上模擬攻撃)結果を「システム設計対策」として整理。

RM の分析結果は、情報システムの受発注者双方が、共通の問題認識と「システム設計対策」をもとに必要な発注要件を具体的に特定できることを想定している。

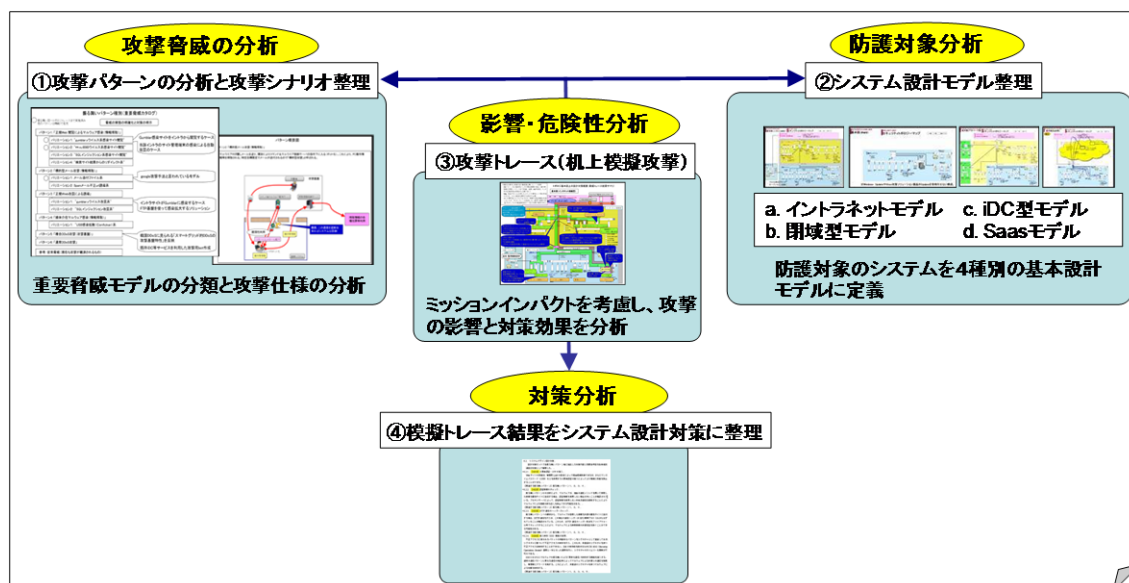



図 4.10-4 RM の分析アプローチ

RM の前提とするサイバー攻撃の基本モデルは以下であり、対策設計思想の前提となっている。

様々な攻撃モデルパターンを分析した結果、いずれの攻撃も第１～３段の攻撃段階を有しており、各パターンほぼ共通的に組織へのミッションインパクト部分は、第３段階の攻撃成否に存在している。

このため、従来対策の範囲である第１段攻撃への対策限界を考慮し、第３段階攻撃の影響回避を視点とした設計管理対策を案出したものである。

ＲＭでは、従来対策とは別に「組織業務への最終影響回避」のための設計対策として整理した。

昨今のサイバー攻撃による組織的影響(ミッションインパクト)の回避には、脅威の再定義と設計思想や組織運用コンセプトの再分析が必要となる。

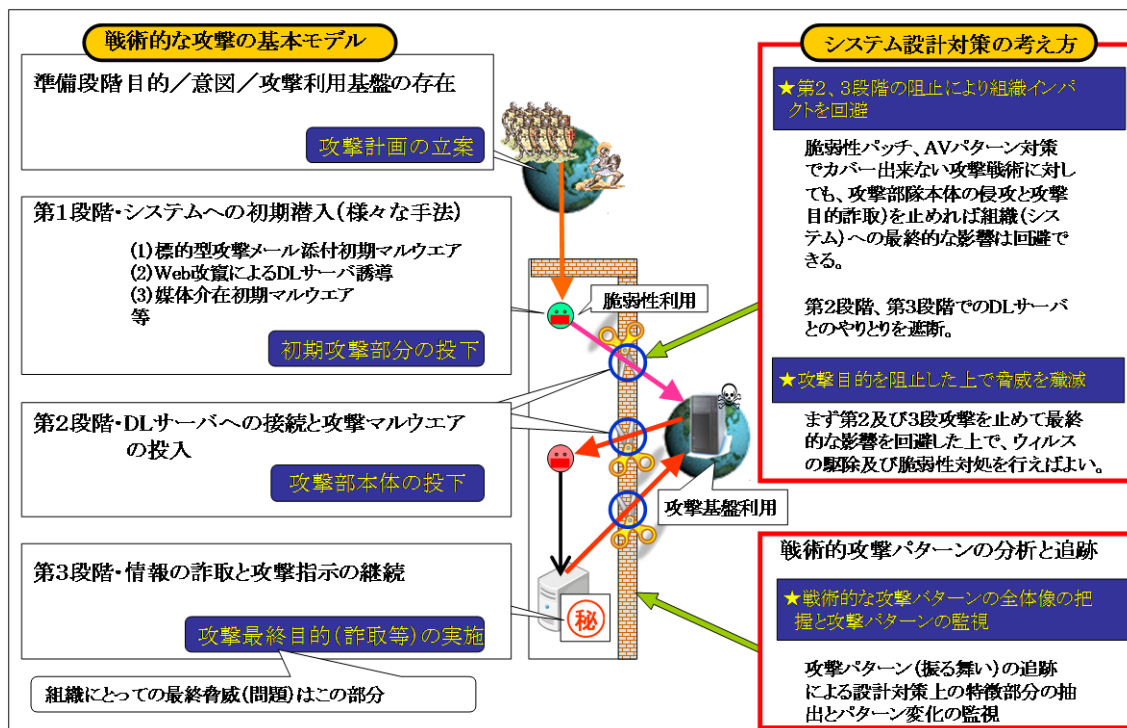



図 4.10-5 RM の前提とするサイバー攻撃の共通基本モデル

4.11.グリーン IT 導入の考え方

グリーン IT とは、環境に配慮した上で情報技術の活用を行う考え方である。日本では 2001 年 1 月に施行された循環型社会形成推進基本法の枠組みを基本として資源リサイクル、エネルギー利用効率向上を目指した法令が成立・改正されており、情報システムに係る政府調達においても、社会の模範となる環境負荷削減への積極的な取り組みにより環境負荷削減を実現することはもちろん、今後は機器統合や省電力機器、および省電力技術の採用、またデータセンタ設備における冷却や電源供給の最適化など通して、消費電力の削減に一層資することが期待されている。

グリーン IT の考え方は、「IT における環境配慮」(Green of IT)と「IT による環境配慮」(Green by IT)の 2 つに大別される。前者は情報システムにおいて導入される機器によって生じる環境負荷を削減する考え方であり、主として物品調達において検討すべき事項となる。後者は情報システムを積極的に活用することにより既存の業務、社会活動や社会システムの環境負荷を削減する考え方であり、情報システムに係る政府調達では、主として企画工程において検討すべき事項となる。

情報システムに係る政府調達においても、社会の模範となる環境負荷削減への積極的な取組により環境負荷削減を実現する″ことはもちろん、今後は機器統合や省電力機器、および省電力技術の採用、またデータセンタ設備における冷却や電源供給の最適化など通して、消費電力の削減に一層資する″

ことが期待されている。

4.11.1.物品調達におけるグリーン IT の考え方

物品調達におけるグリーン IT では、「IT における環境配慮」(Green of IT)が主たる対象となる。特に購買・調達プロセスにおける総合的な取り組みとして、グリーン IT に関して優れた取り組みを行っている製品による応札を優遇する「国等による環境物品等の調達の推進等に関する法律(平成十二年五月三十一日法律第百号) 改正　平成十五年七月十六日法律第百十九号 」及び「環境物品等の調達の推進に関する基本方針(平成二十二年二月五日　変更閣議決定)」(以下　グリーン購入法)が定められている。この法律により国、独立行政法人等、地方公共団体及び地方独立行政法人では特定調達品目においてはグリーン購入法の適合条件を満たしていることが調達条件となっている。 特定調達品目とTRM における技術ドメインの関係は以下に示す通りとなっており、グリーン購入法適合条件は、5 章　各技術ドメインにおける非機能要件の基本項目として記述される。また、グリーン購入法以外に個々各技術ドメインにおいて、標準化されているグリーン IT 技術が存在する場合は、5 章　各技術ドメインで非機能要件の基本又は加点項目として記述する。

平成 21 年度 グリーン購入法 特定調達品目	平成 22 年度 情報システム調達のための技術参照モデル(TRM) 技術ドメイン
電子計算機	5.6.3　サーバハードウェア
	5.8.2　パーソナルコンピュータ
磁気ディスク装置	5.7.1　ディスクストレージ
プリンタ	5.8.6　オフィスプリンタ装置
デジタル印刷機	5.8.6.2　複合機
コピー機(複合機)	5.8.6.2　複合機

ディスプレイ	5.8.2　パーソナルコンピュータ

4.11.2.役務調達におけるグリーン IT 導入

物品調達におけるグリーン IT の中心となる「IT における環境配慮」(Green of IT) では短期的な環境負荷削減効果が期待できる反面、中長期にわたる大きな環境負荷削減効果は困難である。「IT による環境配慮(Green by IT)」は、既存の業務、社会活動や社会システムにおける改革を通じて環境負荷を削減することにより、低環境負荷社会を実現するためのより大きな環境負荷削減効果が期待され、今後さらに積極的な取り組みが求められる分野である。

具体的には、BI の活用等を通じて既存業務で必要となる紙の使用を削減する(紙の削減による環境負荷削減)ことや、電子会議の活用によって職員の地理的移動 を削減する(自動車の走行削減による環境負荷削減等)こと等が「IT による環境配慮」の実現例として挙げられる。 またクラウドサービス では、IT 機器の削減という「IT における環境配慮」と調達や運用負荷の削減という「IT による環境配慮」の両面の利点がある。

また、データセンターの利用にあたっては、IT 機器のエネルギー効率と、冷却等の付帯設備のエネルギー効率の両者を考慮して調達を行うことを検討すべきである。

4.12.IPv6 対応上の留意点

インターネットに接続する上で必要となる IPv4 グローバルアドレスは、新規に割り当て可能な IPv4 在庫アドレス数が枯渇し、新規のアドレス割り当てができない状況である(新規割り当てのグローバルアドレスは IPv6 になる)。そのため、通常は新たな IPv4 グローバルアドレスを持ったサーバの増設や新たな DMZ の構築はできない。また、IPv6 は IPv4 と互換性がないため、単純には IPv6 と IPv4 のネットワークやサーバ間では通信できない。そのため、新たなアドレス割り当てや接続に対応するための IPv6 用環境と既存の IPv4 用環境の共存や併用の対策が必要となる。

この IPv4 と IPv6 の共存や併用が適切に行える様、インターネットに接続するネットワークやサーバ、PC 等の各種機器に関して、設計時及び機材調達時のみならず、運用・管理・監視・保守等の内容やセキュリティ対策についても、あらかじめ考慮しておくことが必要である。

参考文献:「電子政府システムの IPv6 対応に向けたガイドライン」
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070402_5_bt1.pdf　など

5. 技術ドメイン解説

本章では、調達者の視点から各技術ドメインを解説し、政府情報システムの一般的な要件を想定して調達仕様書に書くべき要件の記述例を示している。実際の調達に際しては調達ごとの個別事情を考慮する必要があるので、本章に示された要件を調達仕様書に活用する際には、下記に挙げるカスタマイズを行わなければならない。

｛ ｝(波括弧)でくくられた語句は、調達を行う情報システムごとに異なる可変要素であるので、実際の情報システムの要求に合わせて適切に置き換える。

【 】(すみ付き括弧)でくくられた語句は、本文の内容をより明確にするための例示であるので、実際の情報システムの要求に合わせて適切に置き換える。例示の多くは製品名、商標等を参照することになると思われるが、過去に調達を行った資産の活用等、特定の製品のみを明示的に指定する正当な理由が存在しない場合は、必ず複数の製品名、商標等を例示として挙げるものとし、その例示の後に「等」を付け、製品の限定を行わないものとする。正当な理由が存在する場合は、例示を行うことをせず、製品を特定する情報を詳しく記述する。

要件を示す表の基本という標示は、基本的な要件であり、一般的な製品で実装されていることが期待される要件であることを示す標示である。総合評価方式による調達においては、技術点の必須項目としても差し支えない。加点という表示は、必ずしも多くの調達において必須とはいえない、又は必ずしも多くの一般的な製品で実装されているとは限らない要件であることを示す標示である。総合評価方式による調達においては、対象システムの要件として必須ではない場合は、技術点の加点項目とすべきである。選択という標示は、前述の基本に相当する要件のうち、その要件の記述に示された複数の要素のうちいずれか一つ以上を満たすことが要求されるということを示す標示である。

本章に示されている要件表の例にあるこれらの標記は、該当する技術ドメインの一般的な要件を想定して付けられているので、実際の調達仕様書にこの表の内容を引き写し活用する際には、これらの基本、加点、選択の標記を参考として、それぞれの要件を必須項目とするか加点項目とするか検討を行う必要がある。本章で基本と表示された要件の中には小規模システムでは過剰なものがありうるので、設計構築時には注意して選択する必要がある。また、実際の情報システムの要件とはならない要件を削除する、及び要件表の例の中に存在しない実際の情報システムの要件を追加するという調整を行わなければならない。

「関連する技術」という表に列挙されている技術は、調達の際に参照される可能性の高い技術及びオープンな標準の一部を列挙したものである。これらの技術やオープンな標準を調達仕様書の中で参照する際には、その技術に関する十分な知識と注意をもって参照を行わなければならない。安易な丸写しを行うと実現性が乏しくなる(調達対象となる物品の選択肢を甚だしく狭めてしまう、参照するオープンな標準の版の違いにより既存資産の活用に不具合が生じる等の)場合があるので、全体の整合性を念頭に参照を行う必要がある。

5.1.BI/DWH/ETL

5.1.1.定義

適切な意思決定をより素早く行うために、適切な形式、適切なタイミングで、適切なユーザに対して適切な情報を提供するシステムの総称であり、データの検索、参照、蓄積を統合的・汎用的に行うことにより、業務上で扱う各種のデータを保存、取得をしたり、操作、変換をしたりして、業務上での利用や分析を行う仕組みのことである。

また同時に、各種の分析操作画面の利用や帳票作成を行う際の開発工数等を低減させること等に役立つ仕組みでもある。

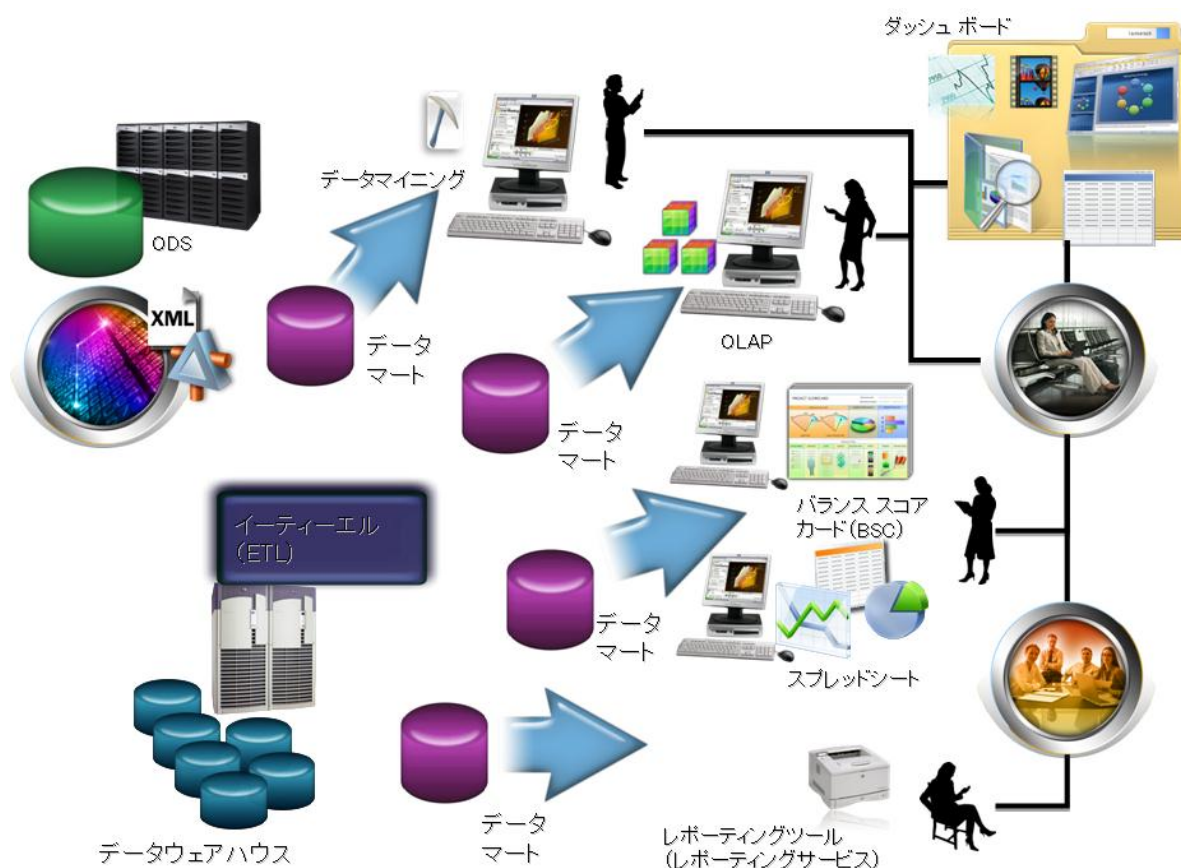



図 5.1-1 ビジネスインテリジェンス概要図

下記にある BI/DWH/ETL の機能・サービスを組み合わせ、選択することにより、例えば下記のような機能やサービスを構築することが可能になる。(以下は、一例となる。)

・ ビジネス パフォーマンス マネジメント

パフォーマンスを最適化し、業務能力の向上を通した生産性向上を実現する。定量、定性的なベンチマークを用いて、業務の効率の測定と監視、及び予測を行う。これにより、傾向やリスクを即座に識別し、タイム

リーなアクションが可能になることを目標としている。

データマートで動作するリレーショナル データベースとスプレッドシート、データマイニング等の分析ツールからなるプラットフォームで構築された統合的なシステム展開により、業務情報や戦略情報の確実な伝達とリアルタイムな業務処理予測と問題追究、ナレッジの活用とコラボレーションによる業務実践といった、一連のマネジメント プロセスをシームレスに接続し、職員のあらゆる活動のサポートを行う。

・　統合財務分析

業務のクリティカルな財務データを安全かつ効果的にあらゆる意思決定者に提供し、費用対効果等の分析を可能にする。

データウェアハウス、ODS とスプレッドシートや OLAP からなるプラットフォームで構築された統合的なシステム展開アプローチで、職員がリアルタイムな意思決定を行い、業務や戦略に従った、生産性の高いスピーディなアクションを可能とする分析システム。データの正確さや高いレベルのセキュリティをも同時に必要とされる。

また、既存の各種統計業務処理を効率化すること等に寄与する。

BI/DWH/ETL の機能・サービス	
機能・サービス	定義
ビジネスインテリジェンス(BI — Business Intelligence)	業務システム等から蓄積される膨大なデータを蓄積・分析・加工して、組織の意思決定に活用しようとする手法。事実に基づくデータを組織的かつ系統的に蓄積・分類・検索・分析・加工して、業務上の各種の意思決定に有用な知見や洞察を生み出すという概念に基づく支援や予測が行える仕組み、活動。又は、そうした活動を支えるシステムやテクノロジ。業務の遂行において必要な情報を自在に分析し、各種の業務向上等に活用することを目指している。
データウェアハウス(DWH — Data Warehouse)	意思決定のため、目的別に編成され、統合化された時系列のデータの集合体であり、基本的には削除や更新の仕組みをもたない。業務システムからトランザクション(取引)データ等を抽出、再構成して蓄積し、情報分析と意思決定を行う。大規模なデータベースを中核とした意思決定支援システム、又は、このようなシステムの構築概念。
イーティーエル ＥＴＬ— Extract/Transform/Load (データ抽出・加工・書き込み機能)	業務システム等に蓄積されたデータを抽出(Extract)し、データウェアハウス等で利用しやすい形に加工(Transform)し、対象とするデータウェアハウス等のターゲットシステムに書き込み(Load)させるという一連の処理のこと。また、これら一連の処理を支援するソフトウェア機能。
データマート	データウェアハウスに保存されたデータの中から、部門や個人の使用目的に応じて特定のデータを切り出して整理し直し、別のデータベースに格納したもので、セントラルのデータウェアハウスが全体業務のデータを統合管理するものなのに対して、特定の部門やユーザの業務ニーズに合わせて必要なデータだけを抜き出したサブセット。
オーラップ OLAP —	エンドユーザが直接データベースの検索・集計を行い、その中から問題点や課題を発見する分析型アプリケーションの概念及びそのシス

Online Analytical Processing(データ集計・分析ツール)	テム。リレーショナル データベースを利用した ROLAP と、多次元データベースを利用した MOLAP、両方式の併用による HOLAP に大別される。
オーディーエス ＯＤＳ — Operational Data Store(一時的データ保存システム)	業務処理系システムのデータ(オペレーショナル・データ)を、検索等別の目的で利用するためにそこから抽出し、一時的にデータを保持したデータの集合体。
データマイニング	種々の解析手法を用いて大量のデータを分析し、隠れた関係性や意味を見つけ出す知識発見の手法の総称、又はそのプロセス。この処理を通じて抽出されたモデルから予測やシミュレーションを行うことが可能となる。
ダッシュ ボード	パーソナライズが行われたポータルへの情報アクセスや分析結果等が情報共有できるツールで、これによりコミュニケーションの一元化を目指している。
レポーティングツール(レポーティングサービス)	業務実績データをサマリーして表示したり、分類、順序付け等を行って表示したりすることで、データについての各種の視点を提供するツール。紙ベース及びインタラクティブな Web ベースの報告書や帳票の作成、管理及び配布等を支援する。
スプレッドシート	数値データの集計・分析に用いられる作表アプリケーションソフト。縦横に並んだマス目(セル)に数値や計算ルールを入力していくと、表計算ソフトが自動的に数式を分析し、所定の位置に計算結果を代入してくれるツール。インタラクティブなクロス集計表等をもち、標準化されたオープンなフォーマットやWebサービス等のインタフェースによりビジネスインテリジェンスのフロントエンドとして利用される。

5.1.2.ビジネスインテリジェンス(BI — Business Intelligence)

業務システム等から蓄積される膨大なデータを蓄積・分析・加工して、組織の意思決定に活用しようとする手法。事実に基づくデータを組織的かつ系統的に蓄積・分類・検索・分析・加工して、業務上の各種の意思決定に有用な知見や洞察を生み出すという概念や予測が行える仕組み、活動。又は、そうした活動を支えるシステムやテクノロジ。業務の遂行において必要な情報を自在に分析し、各種の業務向上等に活用することを目指している。

なお、従来は個別の独立したシステム内のデータ分析が主流であったが、SOA 等のシステム連携基盤の導入に伴い、分散して格納されているデータの同質化を行った上で、データを分析する必要が生じ、メタデータの管理やデータ変換の仕組みをもつことで、これに対応する仕組み(メタデータレジストリ)が、ETL や DWH の組み合わせと、ほぼ同等の機能を提供することになる。

機能要件		
1	基本	データを組織的かつ系統的に蓄積・分類・検索・分析・加工できること。
2	基本	分析によって、有用な知見や洞察を生み出すことが可能な仕組みをもっていること。
3	加点	必要に応じて、【データウェアハウス、ETL、データマート、OLAP、Data Mining 等】を組み合わせられること。
4	加点	必要に応じて、分析結果等の出力を【BSC、ダッシュボード、レポーティングツール、スプレッドシート 等】で選択的に可視化できること。
5	加点	帳票や種々のグラフをインタラクティブに切り替え/連携できる仕組みをもつこと。
6	加点	設定したしきい値によって、適切なユーザにアラートを発信できる仕組みをもつこと。
7	加点	SOA 等のシステム連携基盤の連携データが分析対象のデータとなる場合、メタデータレジストリ(システム間のデータ交換時にメタデータの変換やデータ品質の同質化等を行う)の仕組みをもつこと。

非機能要件(個別の要件がある場合のみ記述)		
バックアップ	加点	データのバックアップ、リカバリ等の機能があること。
セキュリティ	加点	明示的にユーザ ID を特定した上で検索・照会処理を実行するように設定できること。

関連する技術	
メタデータレジストリの形式	ISO/IEC 11179 JIS X4181-3 (, JIS X4181-1, JIS X4181-2) 国際規格の ISO/IEC 11179 に完全に一致する JIS 規格

5.1.3.データウェアハウス(DWH ― Data Warehouse)

意思決定のため、目的別に編成され、統合化された時系列のデータの集合体であり、基本的には削除や更新の仕組みをもたない。データウェアハウスの活用により、業務システムからトランザクション(取引)データ等を抽出、再構成して蓄積し、情報分析と意思決定の支援を行う。大規模なデータベースを中核とした意思決定支援システム、又は、このようなシステムの構築概念。

機能要件		
1	基本	目的別に編成され、統合化された時系列のデータの集合体となっていること。
2	基本	分析等に適した形に加工してない状態のデータ(詳細データ)をそのまま格納して長期間保持できること。
3	基本	トランザクション(取引)データ等を抽出、再構成して蓄積できること。
4	基本	業務システムと独立して構築されること。
5	基本	基本的には更新処理をしないこと。

関連する技術	
DB アクセスインタフェース	SQL

5.1.4. Ｅ Ｔ Ｌ(イーティーエル) ― Extract/Transform/Load(データ抽出・加工・書き込み機能)

業務システム等に蓄積されたデータを抽出(Extract)し、データウェアハウス等で利用しやすい形に加工(Transform)し、対象とするデータウェアハウス等のターゲットシステムに書き込み(Load)させるという一連の処理のこと。また、これら一連の処理を支援する機能。
これを用いることにより、データクレンジング等が可能になる

機能要件		
1	基本	各種のデータソース【標準フォーマットのファイル、データベース、FTP 等】からデータを抽出できること。
2	基本	必要な統合、変換処理【フィルタリング、集計、分割、結合、派生<入力列に式を適用することにより新しい列の値を作成、結果は新しい列として追加するか、既存の列の値を置き換える>、条件分岐　等】ができること。
3	基本	ターゲットとなるシステム【データウェアハウス、データマート　等】にデータをロードさせることができること。
4	基本	各種データフローにおけるエラーイベント等の例外処理ができること。

5	加点	GUI 等により【各種の操作やデータの制御フロー等】が設定、実行できるようになっていること。

関連する技術	
DB アクセスインタフェース	SQL

5.1.5.データマート

データウェアハウスに保存されたデータの中から、部門や個人の使用目的に応じて特定のデータを切り出して整理し直し、別のデータベースに格納したもので、セントラルのデータウェアハウスが全体業務のデータを統合管理するものなのに対して、特定の部門やユーザの業務ニーズに合わせて必要なデータだけを抜き出したサブセット。

機能要件		
1	基本	データウェアハウスに保存されたデータの中から、使用目的に応じて特定のデータを切り出して整理し直し、それが別のデータベースに格納されていること。
2	加点	検索・分析要求に効率的に応じるために要約データとなっていること。

関連する技術	
DB アクセスインタフェース	SQL

5.1.6.OLAP(オーラップ) ― Online Analytical Processing(データ集計・分析機能)

エンドユーザが直接データベースの検索・集計を行い、その中から問題点や課題を発見する分析型アプリケーションの概念及びそのシステム。リレーショナル・データベースを利用した ROLAP(Relational OLAP)と、集計用の多次元データベースを利用した MOLAP(Multidimensional OLAP)に大別される。また、前処理が速くスケーラビリティも考慮した HOLAP(Hybrid OLAP)も存在する。

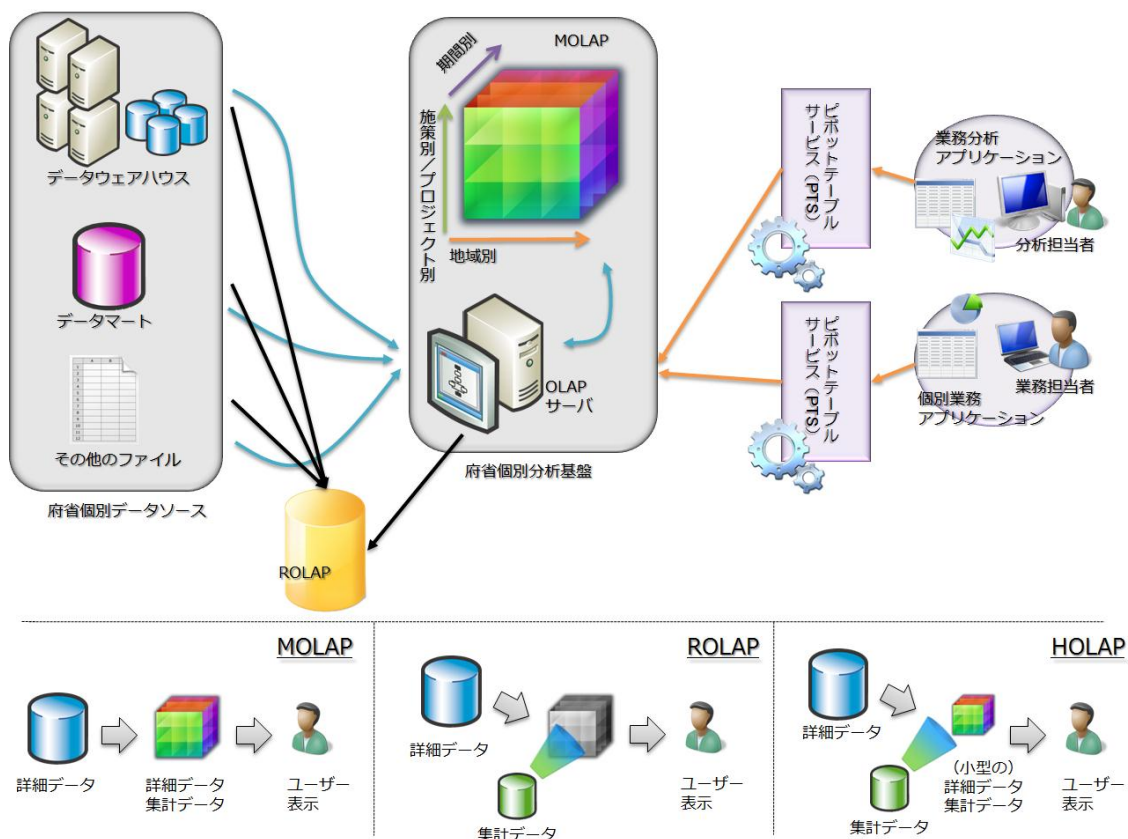



図 5.1-2 OLAP 概要図

機能要件		
1	基本	利用者が直接、データベースの検索・集計を行えるようになっていること。
2	基本	リレーショナル・データベースか、Cube と呼ばれるあらかじめ最適化処理されたデータマネジメントシステム等を用いていること。
3	基本	多次元的な概念ビューをもつこと。
4	基本	【ピボットテーブルサービス(PTS) 等】を介して、レポーティング機能やスプレッドシートからアクセス可能であること。
5	基本	データが格納されている物理的構造を知らなくてもデータに容易にアクセスできること。
6	基本	どの次元、どのセルに対しても【スライシング、ダイシング、ドリリング 等】の機能が、同じパフォーマンスで提供できること。
7	基本	どの次元でも、同じ構造・操作が保証されていること。
8	基本	動的なマトリクス処理ができること。
9	基本	マルチユーザの同時アクセスが可能なこと。
10	基本	クロスディメンション処理にソフトウェアとしての機能上の制約がないこと。

11	基本	柔軟性のあるレポート処理が可能なこと。
12	基本	次元の数やメンバー数に制約がないこと。
13	基本	個々の処理【スライシング、ダイシング、ドリリング　等】がメニューを通さずできること。

関連する技術	
DB アクセスインタフェース	SQL
クエリ言語	MDX(Multi Dimensional Expressions) 多次元データを操作及び取得する際に使用する

5.1.7. ＯＤＳ（オーディーエス） — Operational Data Store(一時的データ保存システム)

業務処理系システムのデータ(オペレーショナル　データ)を、検索等別の目的で利用するためにそこから抽出し、一時的にデータを保持したデータの集合体。

機能要件		
1	基本	業務処理系システムのデータを抽出し、一時的にデータを保持するデータベースになっていること。
2	基本	揮発性をもつリアルタイムデータの格納ができること。
3	基本	短期のデータ保有となっていること。

関連する技術	
DB アクセスインタフェース	SQL

5.1.8.データマイニング

種々の解析手法を用いて大量のデータを分析し、隠れた関係性や意味を見つけ出す知識発見の手法の総称、又はそのプロセス。この処理を通じて抽出されたモデルから予測やシミュレーションを行うことが可能となる。

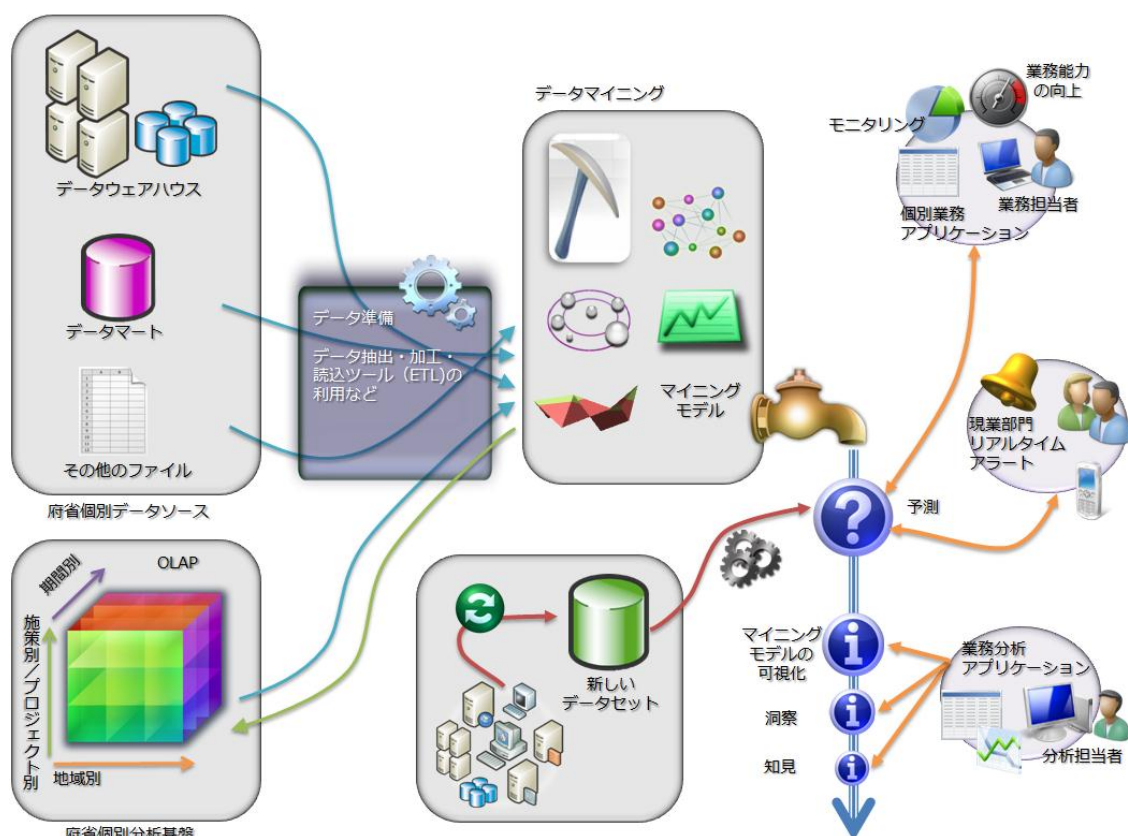



図 5.1-3 データマイニング概要図

機能要件		
1	基本	大量のデータを分析し、隠れた関係性や知見を見つけ出す仕組みをもっていること。
2	基本	関係性や知見を可視化できる仕組みをもつこと。
3	基本	関係性や知見から予測モデルを作成できる仕組みをもち、それを未知のデータへ適用させることで予測が可能な機能をもつこと。
4	基本	予測の確度を検証できる仕組みをもつこと。
5	基本	分析に使用するアルゴリズム【相関ルール、クラスタリング、決定木、ナイーブベイズ、ニューラルネット　等】を選択できる仕組みをもつこと。
6	基本	GUI を用いて、繰り返し、試行錯誤的に分析を行える仕組みをもつこと。
7	加点	【レポーティングツールやスプレッドシート　等】からのアクセスや出力が可能であること。

関連する技術	
DB アクセスインタフェース	SQL

5.1.9.ダッシュ ボード

パーソナライズが行われたポータルへの情報アクセスや分析結果等が情報共有できるツールで、これによりコミュニケーションの一元化を目指している。

機能要件		
1	基本	総合的なポータル フレームワークにより、対象ユーザの特定の要件を満たすポータルサイトを容易に構築できること。
2	基本	各種のサイト【個人サイト、部門別サイト、イントラネット サイト、エクストラネット サイト、及びインターネット サイト 等】を構築可能なこと。
3	基本	オーサリングツールをもち、コンテンツの投稿が容易なこと。
4	基本	対象ユーザの設定機能により、特定のユーザに情報を提供する方法、タイミングや場所を情報の所有者が決められる仕組みをもつこと。
5	基本	提供する情報をパーソナライズ可能になっていること。
6	基本	総合的なアプリケーション統合フレームワークをもち、コンポジット アプリケーションを構築可能であること。
7	基本	アプリケーション ガバナンス機能をもち、アプリケーションの実行環境を詳細に制御できること。

5.1.10.レポーティングツール(レポーティングサービス)

業務実績データをサマリーして表示したり、分類、順序付け等を行って表示したりすることで、データについての各種の視点を提供するツール。紙ベース及びインタラクティブな Web ベースの報告書や帳票の作成、管理及び配布等を支援する。

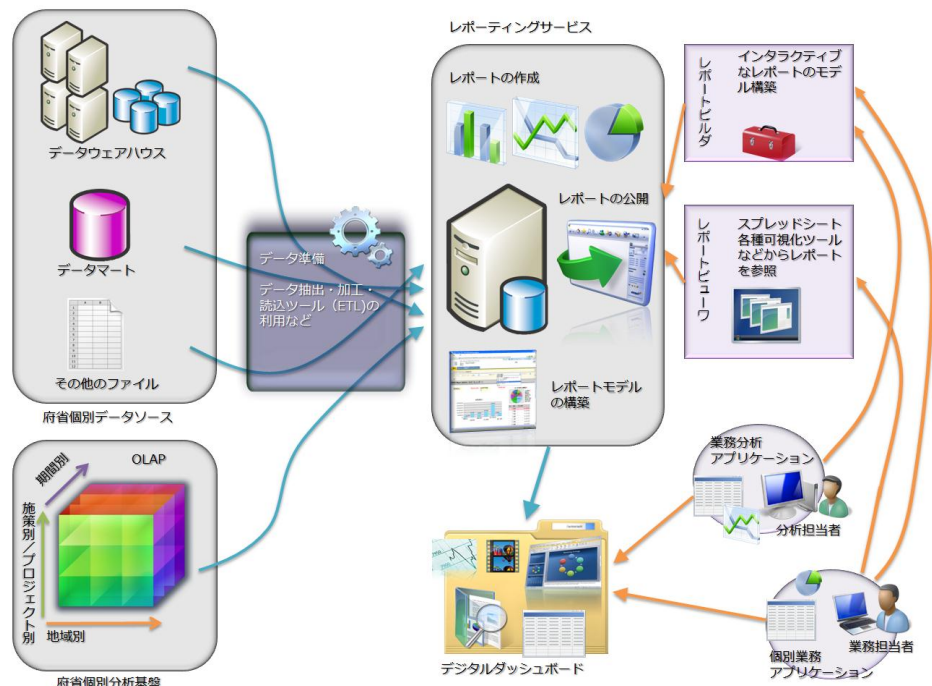



図 5.1-4 レポーティングツール概要図

機能要件		
1	基本	【サマリーや分類、順序付け　等】を行って、利用者が理解しやすい可視化が可能となっていること。
2	基本	レポートの作成のために、データソースへのアクセス設定ができるようになっていること。
3	基本	レポート作成機能やひな形の提供、レポート管理画面が提供されること。
4	基本	紙ベース及びインタラクティブな Web ベースの報告書にも対応していること。【帳票の作成、管理　等】ができること。
5	基本	閲覧者を設定して、レポートの公開や配信が可能となっていること。

5.1.11.スプレッドシート

数値データの集計・分析に用いられる作表アプリケーションソフト。縦横に並んだマス目(セル)に数値や計算ルールを入力していくと、表計算ソフトが自動的に数式を分析し、所定の位置に計算結果を代入してくれるツール。インタラクティブなクロス集計表等をもち、標準化されたオープンなフォーマットや Web サービス等のインタフェースによりビジネスインテリジェンスのフロントエンドとして利用される。

機能要件		
1	基本	OLAP やデータマイニング、(あるいは BI 全般)のフロントエンドとして機能すること。
2	基本	マクロ等により自動処理や制約条件等を埋め込み可能なこと。

5.8.5 共通オペレーションの定義及び 5.8.5.8 表計算の機能要件を参照のこと。

5.2.EAI

5.2.1.定義

EAI(Enterprise Application Integration) とは、多種多様なコンピュータシステム群や各種ビジネスパッケージ群をハブ＆スポーク型のアーキテクチャにて連携/統合させ、より戦略的な機能や情報として提供する機能及びミドルウェア/アプリケーションパッケージや統合技術のことである。

従来サーバ間で情報交換する手法としては、ファイル転送もしくはメッセージング技術が一般的に考えられる。しかし情報交換が必要なサーバ数が増加するにつれ、その情報交換の仕組みを個別に開発運用保守するよりも、その機能を独立させ標準化することが、開発運用保守を考えると効率的であると考え出されたのが EAI である。EAI の処理は非同期処理(疎結合)でなされる形式が一般的である。これはサーバ側の処理、及び EAI 機能サーバの処理を独立的に非同期で処理させることにより、EAI の処理が滞ることで、接続する各サーバの処理に影響が及ぶことを防止するためである。

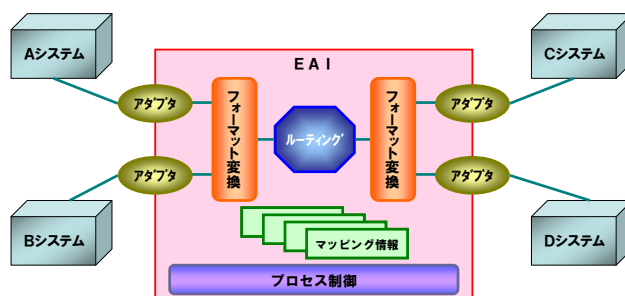



図 5.2-1 EAI の概念図

EAI の機能・サービスの定義	
機能・サービス名	定義
EAI 機能	多種多様なコンピュータシステム群や各種ビジネスパッケージ群をハブ＆スポーク型のアーキテクチャにて有機的に連携／統合させ、より戦略的な機能や情報として提供する。 なお、システム接続のために、ビジネスパッケージ群との接続性を容易にするアプリケーションアダプタ、標準的なプロトコルを使った接続性を容易にするテクノロジアダプタ、汎用機との接続性を容易にするメインフレームアダプタの 1 種類もしくは複数種類のアダプタ機能を提供する。

5.2.2.機能要件

機能要件		
1	基本	接続するシステムやアプリケーションごとの異なるデータフォーマットや文字コードを変換し、対応付けるフォーマット変換機能を有すること。
2	基本	データの内容に応じて、一つ又は複数の送信先へデータを振り分けるルーティング機能を有すること。
3	基本	EAI に接続するサーバ側のインタフェース開発負荷を軽減するために用意される各種接続補助機能(アダプタ)を有すること。
4	基本	ルーティング、フォーマット変換等を組み合わせ、複数のシステムを介した業務プロセスを自動化するプロセス制御機能を有すること。
5	基本	各システムで扱うデータの項目同士を対応付けるマッピング機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
メタデータ定義の提供	加点	業界標準のフォーマットのメタデータ定義を提供する。例えば SWIFT, FIX, EDIFACT 等である。提供されたメタデータ定義を利用することにより、ユーザは一からメタデータを作成せずに済み、開発工数を大きく削減させることが可能になる。
開発環境	加点	多くの EAI ミドルウェアでは独自の開発環境を提供する。そこではプログラム言語でコーディングするのではなく、GUI による drug & drop やビルトイン関数により、直観的な開発を行うことができる。プログラミング言語に精通していないメンバーでも開発が可能であり、高い開発生産性と、保守性(メンテナンスの容易性)を確保できる。

5.3.iDC・設備

5.3.1.定義

iDC(インターネット・データセンター)・設備とは、高速な通信回線が引き込まれ、自家発電設備や高度な空調設備、並びにセキュリティが確保された、耐震性に優れた施設と設備のことである。そこに業務システムが稼動するサーバやネットワーク機器類(以下、機器等)を設置し、インターネット接続サービスを行うとともに、機器等並びにアプリケーション等の稼動監視や障害対応等の運用作業を行うものである。

提供されるサービスとしては、ハウジングサービス、ホスティングサービスに大別される。ハウジングサービスは、ユーザ(利用者)が所有する機器等を iDC で預かり、インターネットへの接続や運用作業を提供するものである。それに対し、ホスティングサービスは、インターネットに接続した機器等を貸し出す(専用もしくはほかの利用者と共用で機器等を貸し出す)サービスであり、そのもとで運用作業の提供を受けるもので、Web サーバやメールサーバとして利用するのが一般的である。

なお、ハウジングサービスの場合は、機器等は別途調達されることから、その諸元を提示する必要があるが、通常、機器等はラックに搭載された形で設置されることから、機器等搭載後のラックの諸元を提示することとなる。提示が必要となる諸元としては、ラックの寸法、ラックの本数、ラックの重量(機器等搭載後の総重量)、ラックの消費電力(機器等搭載後の最大消費電力)、ラックの発熱量(設置するすべての機器の発熱量)、電源(電圧、コンセント形状、コンセント数)である。

また、iDC と府省庁舎との接続や iDC のインターネット接続といった通信回線(通信回線の監視業務を含む)は別途調達として整理し、対象外とした。

iDC・設備の機能・サービス	
機能・サービス	定義
立地条件	地震等の災害により iDC 自身が被害を受けサービスが停止するような事態に陥らないための、iDC の所在に関する条件のことである。
施設・マシンルーム条件	施設条件とは、地震等の災害により iDC 自身が被害を受けサービスが停止するような事態に陥らないための、耐震等の建物の構造や通信設備等の二重化といった条件のことである。 また、マシンルーム条件とは、機器等を搭載したラックを設置する環境(場所)に関する条件のことである。
電源・空調条件	電源・空調設備の障害により、機器等(そのサービス)が停止するような事態に陥らないための、電源・空調設備の二重化といった冗長性確保に関する条件のことである。
セキュリティ条件	iDC への不法侵入や妨害破壊行為、iDC 内の情報資産への不正アクセス等を未然に防止するための物理的セキュリティに関する条件であり、機器等のセキュリティ対策等の作業については、別途調達される運用業務の範ちゅうとした。 運用業務に関しては、「5.9. 運用管理/セキュリティ」を参照のこと。
運用条件	iDC・設備の維持・管理作業に関する条件であり、機器等の稼動監視や構成、障害管理やバックアップ取得等の作業について

	は、別途調達される運用業務の範ちゅうとした。 運用業務に関しては、「5.9. 運用管理/セキュリティ」を参照のこと。

5.3.2.立地条件

立地条件は、iDC の所在に関する条件のことである。

機能要件		
1	基本	地震による被害の恐れの少ない地域であること。(文献で指摘された活断層直近にないこと、及び文献に記載された過去に液状化被害を受けた地域でないこと。)
2	基本	国土交通省や自治体が公開しているハザードマップ等の情報で危険地域と指定された場所にないこと。
3	基本	津波、高潮、集中豪雨等による出水の危険性を指摘されていない地域であること。
4	基本	半径{100}m 以内に消防法における指定数量以上の危険物製造施設や高圧ガス製造施設がないこと。
5	基本	障害発生の際に、機器等の保守業者のサポート拠点から{30}分以内でアクセス可能であること。

5.3.3.施設・マシンルーム条件

施設条件は、耐震等の建物の構造や通信設備等の二重化といった条件のことであり、マシンルーム条件とは、ラック・機器を設置する環境に関する条件のことである。

機能要件		
1	基本	建物構造が震度{6 強}に耐えうる耐震、あるいは免震等の構造を備えていること。
2	選択	建築基準法及び消防法に適合した火災報知(防災)システムが設置されていること。 もしくは、建築基準法及び消防法に適合した火災報知(防災)システム、あるいは室内環境の変化を敏感に察知し火災予兆を検知できるシステムが設置されていること。
3	選択	消火設備は、消火時の水害、並びに環境保護を考慮したオゾン層破壊係数がゼロであるガス系消火設備とすること。 もしくは、消火設備は、消火時の水害、環境保護、並びに人体への影響を考慮し、窒素消火設備とすること。
4	基本	避難経路を複数確保する観点で、建物への出入り口を{2}箇所以上設けていること。 また、ラック、機器等の搬出入のためのエレベータが設置され、24 時間×7 日間／週利用可能であること。
5	基本	通信回線については、特定の通信事業者に依存しない経路の異なった{2}系統以上の回線の引き込みができること。
6	基本	マシンルームは無窓とする等、外部から内部が見通せない構造とすること。
7	基本	マシンルームのフリーアクセスは、最大加速度{500}gal 以上に耐えうること。ただし、免震構造の場合は建物もしくは免震装置・床が当該加速度以上に耐えうること。
8	基本	マシンルームの天井高はフリーアクセス床を除いて{2,400}mm 以上であること。
9	基本	マシンルームのフリーアクセスの床荷重は、別途調達される機器及び機器搭載後のラックの重量{600}kg/㎡以上に耐えられる能力を有していること。
10	基本	マシンルームは、防火区画されていること。

11	基本	セキュリティ管理上、ほかの iDC 利用者と混在しない独立した区画を提供すること、あるいはほかの iDC 利用者と混在しないようラック単位に施錠できること。
12	基本	別途調達されるラック、機器等の諸元表に記載する設置環境(機能)を提供すること。

非機能要件（個別の要件がある場合のみ記述）		
環境要件	基本	環境マネジメントシステムの国際規格であるISO14001の認証を取得していること。

5.3.4.電源・空調条件

電源・空調条件は、電源・空調設備の二重化といった冗長性確保に関する条件のことである。

機能要件		
1	基本	受電設備は法定点検時も完全無停止であること。
2	基本	無停電電源装置(UPS)や定電圧定周波数装置(CVCF)、自家発電装置を備えていること。また、発電設備使用中も燃料補給にて継続運転を可能とし、完全無停止であること。
3	基本	{2}系統以上の給電経路・方式にて電源の引き込みを図り、施設内は二重化等の冗長性を確保していること。
4	基本	二重化等の冗長性を確保した空調設備を有していること。 また、災害時に断水となっても{24}時間以上連続して運転可能な空調設備であること。
5	基本	別途調達されるラック、機器等の諸元表に記載する電源設備(機能)を提供すること。
6	基本	別途調達されるラック、機器等の諸元表に記載する空調設備(機能)を提供すること。

5.3.5.セキュリティ条件

セキュリティ条件は、物理的セキュリティに関する条件である。

機能要件		
1	基本	建物への入館とマシンルームへの入室に係るセキュリティ認証機能がそれぞれ独立した仕組みであること。また、建物の入り口において有人警備を含むセキュリティ対策が施されていること。
2	基本	【侵入検知センサー、監視カメラ、入退室管理システム　等】による機械警備システムが導入されていること。
3	基本	常駐警備員又は機械警備システム等による入退管理が 24 時間×7 日間／週されていること。
4	基本	iDC 内の入退管理方式として、IC カードや生体認証装置等の本人確認装置を有するとともに、監視カメラが共用部やサーバルーム等に設置されていること。

非機能要件（個別の要件がある場合のみ記述）		
セキュリティ評価・認証要件	基本	財団法人日本情報処理開発協会が定める「情報セキュリティマネジメントシステム(ISMS)適合性評価制度(JIS Q 27001, ISO/IEC27001)」の認証を取得していること。かつ、プライバシーマーク使用許諾事業者であること。

5.3.6.運用条件

運用条件は、iDC・設備の維持・管理作業に関する条件である。

機能要件		
1	基本	iDC・設備に係る 24 時間×7 日間／週の管理体制を提供するとともに障害等の受け付け・連絡窓口を開設していること。
2	基本	iDC・設備の定期点検を実施していること。

5.3.7.仮想化への対応

機能要件		
1	基本	仮想化機構により実現された仮想化ゲストサーバ、仮想化ストレージ、仮想化ネットワークなどから構成される仮想化環境において物理サーバ環境と同等のソフトウェアを配置でき、同等の機能を満たすことができること。

5.4. SOA 関連機能

5.4.1. 定義

5.4.1.1. SOA(Service Oriented Architecture)

業務上の一つの処理に相当するソフトウェアの機能をサービスと見なし、そのサービスをネットワーク上で標準化された手順で呼び出せるように連携させてシステム全体を構築していくアーキテクチャ。現在、一般的には Web サービス技術仕様を用いることが多い。サービスのインタフェースを定義し、ネットワーク上で連携させてシステム全体の素早い構築及び高いメンテナンス性を可能にする仕組みでもある。

図 5.4-1 SOA 主要コンポーネント

SOA の機能・サービス	
機能・サービス	定義
ビジネス・プロセス管理 (Business Process Management)	複数のサービスの組み合わせやフロー制御を定義することでサービスとビジネス・プロセスを結合し、ビジネス・プロセスの実行を支援する。
エンタープライズ・サービス・バス(Enterprise Service Bus)	分散アプリケーション間のインタフェースを隠蔽することで、サービス相互の独立性を高め、メッセージの信頼性を保証することにより、サービスの統合を実現する。
マネジメント(Management)	サービスを仲介し、セキュリティ及びポリシーを管理する。
マッシュアップポータル (Mashup Portal)	フロントエンドゲートウェイとしてサービスをマッシュアップして提供する。
ビジネス活動監視 (Business Activity Monitoring)	業務及びプロセスを監視し、SLA や KPI(Key Performance Indicators：重要業績評価指標)と実際のビジネス・プロセスとを関連付け、可視化する。

開 発 環 境 (Development Environment)	SOA サービス開発のための IDE 及びアプリケーション開発フレームワークを提供する。
サービス・リポジトリ/レジストリ(Service Repository/ Registry)	SOA サービスに関する情報の登録、公開、検索により、サービスのライフサイクル管理を実現すると同時に、業務アプリケーションによる動的なサービス呼び出しを可能にする。
アダプタ(Adapters)	Web サービスやレガシーシステム、データベース、ERP、バックエンドシステム、カスタムアプリケーション及びサービス等との接続を実現する。
Web サービスプロトコル (Web Services Protocol)	インターネット標準技術を使用して、異なるプラットフォーム上のアプリケーションを統合することを可能にする仕組みを提供する。詳しくは、「Web サービスプロトコルの機能・サービス」参照。

この中で、エンタープライズ・サービス・バスは、アプリケーションの統合を実現するためのメッセージング、データ変換機能を提供する。個別のサービスを取りまとめるビジネス・プロセス管理は、アダプタ(Web サービスプロトコルを含む)を介し、サービスの組み合わせ及び実行制御を行うことによって業務アプリケーションを実現する。ビジネス活動監視は、ビジネス・プロセス管理からパフォーマンスデータやアラート情報を収集して業務プロセスの情報を可視化した状態で提供する。また、マッシュアップポータルは、ビジネス・プロセス管理からコンテンツやデータを受け取り、利用者にマッシュアップしたコンテンツを提供するなど、システム利用者への情報提供が実現される。サービス・リポジトリ/レジストリに格納された SOA サービスの情報をもとにマッシュアップ開発を容易にする開発環境も提供される。

システム管理者や開発者など提供者側にとっても、SOA のマネジメント機能によって、サービスのログ情報や監視統計情報を収集したり、アクセス・ポリシーの設定を行う等の管理を行ったりができ、さらに開発環境によって、インタフェースとサービスを分離した変化に強いアプリケーションの開発のための統合環境が提供されるため、開発が容易になる。

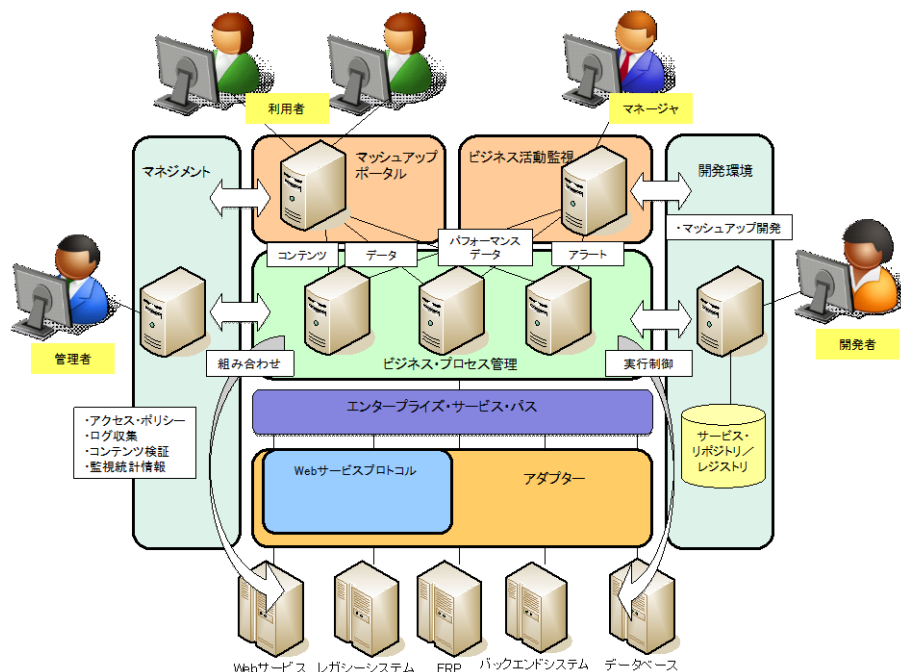



図 5.4-2 SOA コンポーネント間の関係

5.4.1.2. Web サービスプロトコル

インターネット標準技術を使用して、ネットワーク上に分散したアプリケーションを連携させる技術の総称であり、異なるプラットフォーム上のアプリケーションとも統合することを可能にする仕組み。 また、このようにして実現される複数の Web サービス同士をつなぎ合わせて新たなアプリケーションやサービスを構築することを可能にする仕組みでもある。

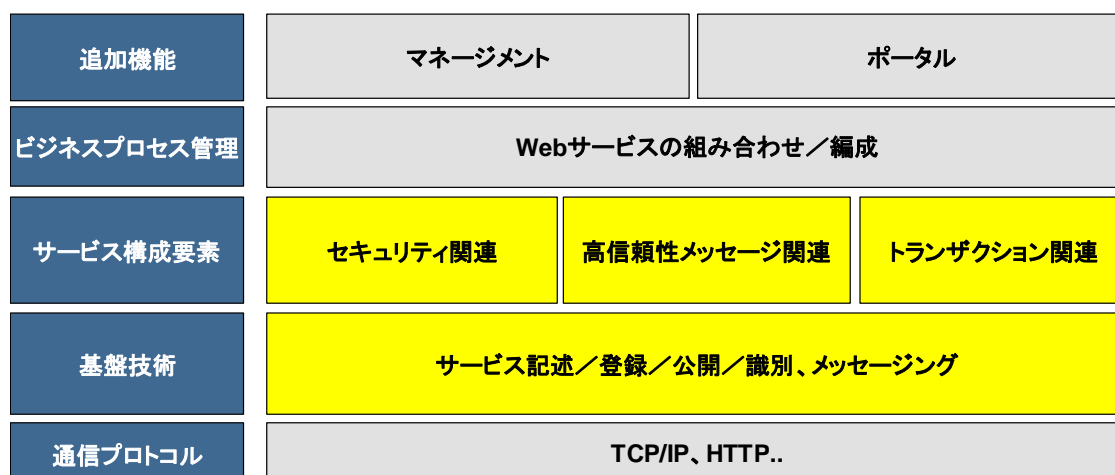



図 5.4-3 Web サービス技術の基本要素

Web サービスプロトコルの機能・サービス	
機能・サービス	定義
基盤技術	Web サービスがどのような機能をもつのか、それを利用するためにはどのような要求をすればよいのか等、サービスを記述し、公開する。また、公開された Web サービスを識別し、その Web サービスとの間でメッセージの交換を行う。
セキュリティ関連サービス構成要素	セキュリティ関連の組み合わせ可能なサービス構成要素であり、メッセージ内容の完全性と機密性を実現するために Web サービスを拡張する。
高信頼性メッセージ関連サービス構成要素	高信頼性が保証されるメッセージ関連の組み合わせ可能なサービス構成要素であり、分散アプリケーション間でのメッセージ信頼性を向上させるために Web サービスを拡張する。
トランザクション関連サービス構成要素	トランザクション関連の組み合わせ可能なサービス構成要素であり、分散アプリケーション間のトランザクションを実現するために Web サービスを拡張する。

5.4.1.3. 共通技術標準

SOA、Web サービスプロトコルを支える共通の技術標準仕様が存在する。この標準仕様によって相互運用性の高い機能、サービスが実現する。

共通技術標準の機能・サービス	
機能・サービス	定義
共通技術標準	SOA、Web サービスプロトコルの前提となる技術標準である。

5.4.2. ビジネス・プロセス管理

機能要件		
1	基本	ビジネス・プロセスのデータや制御フローを定義するために必要なデータ操作機能を提供していること。
2	基本	サービスの呼び出し、データ操作、障害通知、例外処理、プロセスの終了などを組み合わせたプロセスを定義できること。
3	基本	サービスとのやり取りを行うための標準(Web サービスプロトコルなど)又は実装規約に基づいて管理が行えること。

非機能要件(個別の要件がある場合のみ記述)		
バックアップ	加点	ビジネス・プロセス構成情報のバックアップを取得すること。

5.4.3. エンタープライズ・サービス・バス

機能要件		
1	基本	特定のネットワークトランスポート技術に依存しない構造で異なるシステム間をつなぐ共通バックボーンを提供すること。
2	基本	異なるプロトコル間の変換が可能なこと
3	基本	異なるデータ形式の間で変換が可能なこと
4	基本	メッセージ内容によるルーティングが可能なこと
5	基本	分散アプリケーション間において、アプリケーションやネットワークで障害が発生した場合、トランザクションをロールバックしてエラー通知を行ったり、エラー解決後トランザクションを再送信するための、メッセージを確実に伝達したりする仕組みを提供すること。
6	基本	エンタープライズ・サービス・バスを利用するほかの要素の処理を変えることなく独立して使用できること。

非機能要件(個別の要件がある場合のみ記述)		
バックアップ	加点	サービス連携に関する設定情報のバックアップを取得すること。

関連する技術	
XML 照会言語	XQuery – XML データの照会言語。
XML 変換言語	XSLT – XML データの変換指定を記述する言語。

5.4.4. マネジメント

機能要件		
1	基本	サービス操作を制御するポリシー(アクセス・ポリシー、ログ収集・ポリシー、コンテンツ検証など)及びアクセス状況や実行状況の監視を定義できること。
2	基本	既存のサービスを変更することなく、アクセス・ポリシーなどを実現できること。
3	基本	監視統計情報を一元管理し、可視化できること。

非機能要件(個別の要件がある場合のみ記述)		
バックアップ	加点	ポリシー設定情報及び監視統計情報のバックアップを取得すること。

5.4.5. マッシュアップポータル

機能要件		
1	基本	複数のサービスインタフェースを組み合わせ、一つのポータルアプリケーションとして構築する機能を提供していること。
2	基本	従来のアプリケーションのビジネスロジックを変更することなく、UI だけを自由にカスタマイズできること。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	加点	ポータルアプリケーション構築に関する設定情報のバックアップを取得すること。

5.4.6. ビジネス活動監視

機能要件		
1	基本	業務及びプロセスを監視し、可視化する機能を提供していること。
2	基本	SLA や KPI と実際のビジネス・プロセスとを関連付け、可視化する機能を提供していること。
3	基本	Web を介した業務及びプロセスの監視とアラート通知機能を提供していること。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	加点	ビジネス・プロセスの監視情報のバックアップを取得すること。

5.4.7. 開発環境

機能要件		
1	基本	SOA サービス開発のための統合開発環境(IDE: Integrated Development Environment)を提供していること。
2	基本	SOA サービス開発のためのアプリケーション開発フレームワークを提供していること。
3	基本	SOA サービス開発のためのライフサイクル(モデリング、プログラム開発、デバッグ、テスト、プロファイリング、チューニング、配布)全体をサポートし、IDE から実行可能であること。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	加点	SOA サービス開発のためのライフサイクルで使用するソースコード及び設定情報のバックアップを取得すること。

関連する技術	
設計記法	UML(Unified Modeling Language) – OMG で開発されたソフトウェア開発におけるプログラム設計で用いられるオブジェクト指向に基づいた統一記法である。

5.4.8. サービス・リポジトリ／レジストリ

機能要件		
1	基本	SOA サービスに関する情報の標準ベースの登録、公開、検索の仕組みを提供すること。
2	基本	すべてのコンポーネントに関して、検索・取得・変更・削除に対するアクセス・パーミッションを設定可能であること。
3	基本	公開された SOA サービスを登録、公開、検索する管理インタフェースを提供すること。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	加点	サービス・リポジトリ／レジストリに関する設定情報のバックアップを取得すること。

5.4.9. アダプタ

機能要件		
1	基本	【Web サービス、レガシーシステム、データベース、ERP、バックエンドシステム、カスタムアプリケーション 等】の接続を実現すること。
2	基本	アプリケーション・トランザクション、ワークフロー及び問い合わせアプリケーション・データの同期呼び出しが可能であること。
3	基本	基幹業務アプリケーションからイベントを非同期受信が可能であること。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	加点	接続に関する設定情報のバックアップを取得すること。

関連する技術	
Web サービス記述言語	WSDL (Web Services Description Language) – Web サービスインタフェースを XML 形式で記述するための規約である。
業界標準仕様	ビジネス分野で利用されるデータ形式の各種標準仕様。例えば XBRL(eXtensible Business Reporting Language：財務情報を記述するための XML ボキャブラリ)、UN/CEFACT CCL(Core Component Library：様々な業種の情報項目をコード化したもの)、さらに省庁内で規定されている標準等。

5.4.10. Web サービスプロトコル

5.4.10.1. Web サービスプロトコル(基盤技術)

機能要件		
1	基本	インターネット標準のネットワーク通信プロトコル(TCP/IP や HTTP など)が利用可能であること。
2	基本	XML をベースとしたメッセージ交換及びリモートプロシージャ呼び出しを実現する仕組みを提供すること。
3	基本	Web サービスの開発及びデプロイを実現するための環境を提供すること。
4	基本	Web サービスからのデータ送受信を実現するための仕組みを提供すること。
5	基本	Web サービスがどのような機能をもつのか、それを利用するためにはどのような要求をすればよいのか等を定義できること。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	加点	Web サービスプロトコル処理時に通常の動作プログラムを著しく遅延させない十分な処理能力をもった構成とすること。
バックアップ	加点	Web サービスインタフェースの設定情報のバックアップを取得すること。

関連する技術	
Web サービス通信プロトコル	SOAP (Simple Object Access Protocol) – XML をベースとした、ほかのコンピュータにあるデータやサービスを呼び出すためのプロトコルである。
Web サービス記述言語	WSDL (Web Services Description Language) – Web サービスインタフェースを XML 形式で記述するための規約である。
Web サービス相互運用性プロファイル	WS-I Basic Profile – Web サービスにおける SOAP メッセージ交換、WSDL の記述法などの相互運用性を高めるためのガイドライン。WS-I で策定された V1.1 が現在 ISO 規格。 ISO/IEC 29361::2008 – WS-I Basic Profile Ver1.1 ISO/IEC 29362::2008 – WS-I Attachments Profile Ver1.0 ISO/IEC 29363::2008 – WS-I Simple SOAP Binding Profile Ver1.0

5.4.10.2. Web サービスプロトコル(セキュリティ関連サービス構成要素)

機能要件		
1	基本	メッセージ内容の完全性と機密性を保証する仕組みを提供すること。
2	基本	【デジタル署名の付加、ユーザ認証データ(トークン)の付加、メッセージの暗号化　等】が利用可能であり、セキュリティ保護が実現できること。
3	基本	任意の標準的な署名・暗号化アルゴリズムを選択できる構造となっていること。
4	基本	Web サービスプロトコルのほかの構成要素の処理を変えることなく独立して使用できること。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	加点	署名処理や暗号化処理時に通常の動作プログラムを著しく遅延させない十分な処理能力をもった構成とすること。
バックアップ	加点	メッセージ内容の完全性と機密性に関する設定情報のバックアップを取得すること。

関連する技術	
Web サービスセキュリティ	WS-Security – Web サービスにおけるセキュリティ機能実現のための技術基盤であり、XML 署名や XML 暗号などの既存のセキュリティ技術を SOAP メッセージのヘッダ部分に組み込む方法を規定し、セキュリティ技術を統合する共通基盤を提供する。
セキュリティ通信プロトコル	SSL(Secure Socket Layer) – インターネット上でデータを暗号化しての送受信するプロトコル。

5.4.10.3. Web サービスプロトコル(高信頼性メッセージ関連サービス構成要素)

今後調達要件として検討を要することが予想されるので項目のみ規定する。

5.4.10.4. Web サービスプロトコル(トランザクション関連サービス構成要素)

今後調達要件として検討を要することが予想されるので項目のみ規定する。

5.4.11. 共通技術標準

関連する技術	
XML 記述言語	XML(eXtensible Markup Language) – 構造化された文書やデータを記述するためのマークアップ言語である。
XML スキーマ言語	W3C　XML Schema – XML 文書の構造やデータ型を定義するためのスキーマ言語である。

5.5.保守環境

5.5.1.定義

保守環境(Maintenance Environment) とは、システムの保守・管理を行うための物理的な作業環境である。保守環境は、システムの運用開始後、アプリケーションプログラムの機能追加、サポート期限切れ等に伴う OS、商用ソフトウェア、オープンソースソフトウェア等のソフトウェアバージョンアップに伴う検証のために活用される。具体的には、運用環境(本番環境)も含めた作業手順・方法をまとめた保守プロセス、保守作業で使用するハードウェア、ソフトウェア、保守用ツール(開発ツール)、自動テストツール等を指す。

保守環境は、ソフトウェア開発のためにベンダー等に設置される「開発環境」とは完全に独立した作業環境であり、ソフトウェアの管理・変更・修正等の支援を行うソフトウェアエンジニアリング環境(Software Engineering Environment)、ソフトウェアのテストのためのソフトウェアテスト環境(Software Testing Environment)の 2 つの環境から構成される。

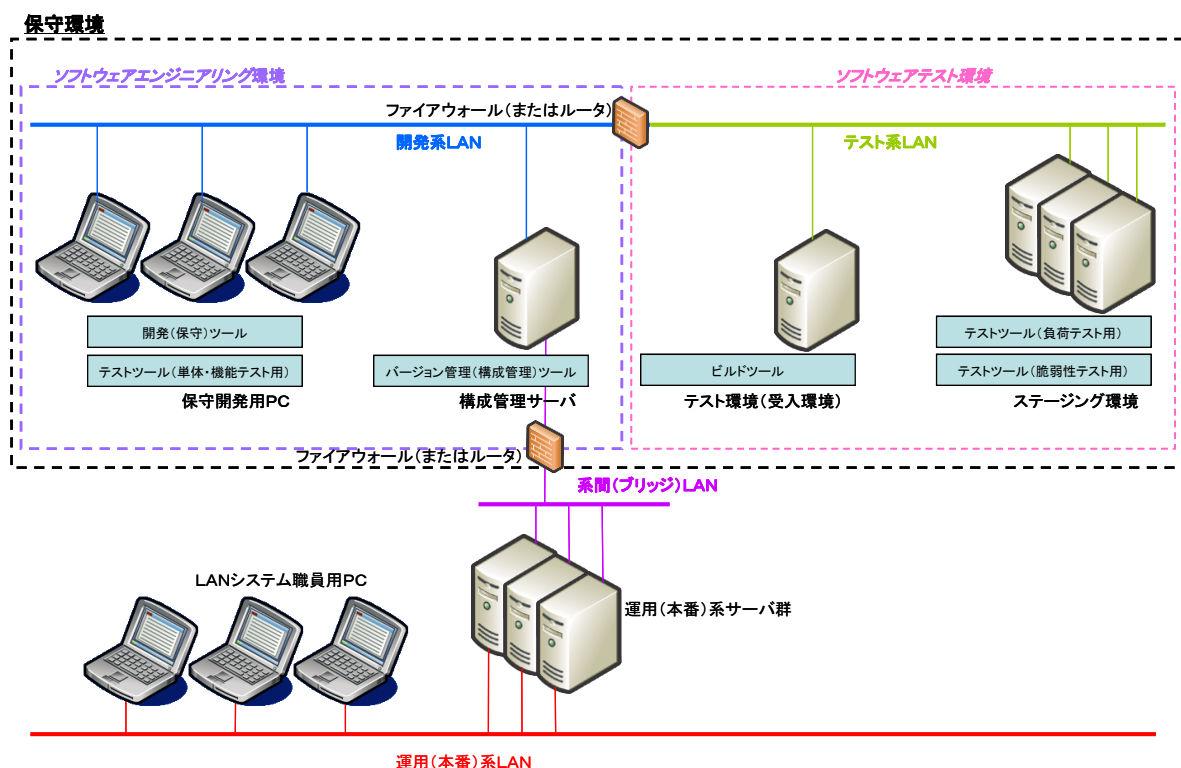



図 5.5-1 保守環境概要図

保守環境の定義は次の通りである。

機能・サービス名	定義
保守プロセス	ハードウェア、ソフトウェア等システムの構成品目(CI)を修正、変更する場合の手順・方法である。
監査プロセス	情報セキュリティ関係規程が適切に運用され、その準拠性と妥当性を確認するための手順・方法である。
開発ツール	開発メソドロジ・プロセスのほか、設計・開発・保守に必要となるツール、又はツール群(統合開発環境:IDE)である。
構成管理・ バージョン管理ツール	度々変更が実施されるアプリケーションプログラムや設計書、手順書等のドキュメントの版(Version)管理を行うためのツールである。 システムのライフサイクルを通して、ハードウェア、ソフトウェア、ファームウェア、ドキュメント等の変更を制御・記録するためのツールである。 開発環境や稼動環境で使用されている構成品目(CI)の情報を一元的に管理し、システムの一貫性を維持するための構成情報を提供する。
開発系 LAN	ソフトウェアエンジニア環境で利用される構内ネットワーク(LAN)である。セキュリティの問題から、運用(本番)環境とは物理的もしくは論理的に分離したネットワークである。
テスト系 LAN	ソフトウェアテスト環境で利用される構内ネットワーク(LAN)である。セキュリティの問題から、運用(本番)環境とは物理的もしくは論理的に分離したネットワークである。
系間(ブリッジ)LAN	開発系 LAN と運用(本番)系 LAN を接続する構内ネットワーク(LAN)である。開発系 LAN・テスト系 LAN と運用(開発)系 LAN の分離が論理的に実現される場合、系間(ブリッジ)LAN はスイッチ、ルータ等の装置で代用されることもある。
テスト環境(受け入れ環境)	委託開発先で単体テストが完了したアプリケーションプログラムのビルド、結合テスト、総合テスト、回帰テスト(リグレッションテスト)を行う検証環境である。
テストツール	保守環境におけるテストツールは、システムの変更時のデグレードや性能劣化を防止するため、回帰テストや性能テスト等のテストを効率的に実施するためのツールである。
ステージング環境	運用(本番)環境と同等のシステム構成(ハードウェア、ソフトウェアとも)のテスト環境である。セキュリティ対策パッチやバグフィックスパッチの運用環境適用前に、パッチ適用時による問題発生の有無を検証する環境である。仮想化されたサーバ、ストレージ上に構築されることもある。

5.5.2.保守プロセスの機能／非機能要件

保守プロセスは、運用(本番)環境、開発環境等ハードウェア、ソフトウェア等の不具合対策や機能変更にあたり、実施すべき作業や手順・方法を定義したものである。

機能要件		
1	基本	開発完了・運用開始時から運用終了・システム廃棄までに実施する作業について、実施する手法・手順がもれなく網羅的に定義されていること。
2	基本	変更要求や変更承認のルールが明確に定義されていること。
3	基本	運用(本番)環境、保守環境それぞれの保守プロセスが定義されていること。

非機能要件（個別の要件がある場合のみ記述）		
整合性	基本	調達計画書、調達仕様書、システム基本設計書等で規定するシステムライフサイクルや要件と矛盾がない保守プロセスが定義されていること。

関連する技術	
IT サービスマネジメント	IT サービスマネジメントは、顧客の要件に適合したレベルの IT サービスの運用管理を実施し、そのサービス品質を継続的に改善するための仕組み。 ISO/IEC 20000、JIS Q 20000、ITIL v.3
ソフトウェア保守	ソフトウェア保守は、問題の発生、改善要求、新環境への適応要求に対応して、ソフトウェア製品のコード及び関連文書を修正する作業。 ISO/IEC 14764、JIS X 0161
ソフトウェア・ライフサイクル・プロセス(SLCP)	ソフトウェア・ライフサイクル・プロセスは、関係者間で、ソフトウェア開発作業に対する相互誤解がないように様々な作業内容の詳細を規定する枠組みのこと。 ISO/IEC 12207、JIS X 0160、共通フレーム 2007
情報セキュリティマネジメント	情報セキュリティマネジメントは、事業リスクの対処方針に基づいて、情報セキュリティの確立、導入、運用、監視、レビュー及び維持改善を行う管理手法。 ISO/IEC27002、JIS Q 27002
ソフトウェアエンジニアリング	ソフトウェアエンジニアリングは、ソフトウェアの開発や保守に関する理論，方法，ノウハウ等を活用したソフトウェア及びソフトウェアの開発・保守作業等の改善活動。 SWEBOK2004(ISO/IEC TR 19759)

5.5.3.開発ツールの機能要件／非機能要件

開発ツールは、主としてソフトウェアの改修や機能強化を行うために使用する統合開発環境(IDE)、開発中のアプリケーションを自動検証するテストツールから構成される。

機能要件		
1	加点	ソースコードレベルのデバッグ機能を有していること。
2	加点	オブジェクト指向言語の利用においては、ソースコードのリファクタリング支援機能を有すること。
3	加点	オブジェクト指向言語の利用においては、テストツールと連携し、テストの自動実行やテスト対象に対応したテストプログラムのひな形を自動生成する機能を有すること。
4	加点	ビルドツールと連携して、コード自動生成等開発作業を自動化する機能を有すること。
5	加点	バージョン管理ツールと連携することにより、チーム開発を支援する機能を有すること。
6	加点	開発用端末単体で動作するローカル環境、ネットワークと接続して開発環境のリソースにアクセスできるチーム環境を切り替えて利用が可能であること。
7	加点	構成管理・バージョン管理ツールとの連携機能を有すること。

8	基本	ソースコードをバイナリコードにコンパイルし、バイナリコードのパッケージ化を行えること。
9	加点	品質向上や生産性向上のため、ビルド作業を自動化やスクリプト化が行えること。

非機能要件（個別の要件がある場合のみ記述）		
整合性	基本	開発で用いた開発言語【C#、Java、C++ 等】、開発フレームワーク【Struts、Turbine、Spring、Hibernate、Seasar2 等の OSS、又は同等の商用製品】に対応していること。（バージョンも含む）

関連する技術	
開発言語	C#　JIS X 3015:2006、ISO/IEC 23270:2006 JAVA　TR X 0005-1:2006 COBOL85　JIS X 3002:1992、ISO/IEC 1989:1985 COBOL2002　ISO/IEC 1989:2002 FORTRAN77　JIS X 3001:1982、ISO/IEC 1539:1980 FORTRAN90　JIS X 3001:1994、ISO/IEC 1539:1991 FORTRAN95　JIS X 3001-1:1998、ISO/IEC 1539:1997 C++　JIS X 3014:2003、ISO/IEC 14882:2003 C　JIS X 3010:2003、ISO/IEC 9899:1999
開発フレームワーク	Apache Struts (1.2.x、1.3.x)、Apache Struts2(2.0.x)-MVC デザインをベースに設計されたアプリケーション・フレームワーク。 Jakarta Turbine - サーブレットベースのアプリケーション・フレームワーク。 バージョン 2.3.x 系が主流。 Spring 2.5.x-小さなコンポーネントフレームワークから構成されるアプリケーション・フレームワーク。 Hibernate 3.3.x-オブジェクトリレーションマッピング・フレームワーク。

5.5.4.構成管理・バージョン管理ツールの機能要件／非機能要件

構成管理・バージョン管理ツールは、システムで使用している構成品目(CI)の情報を一元に管理し、開発から廃棄に至るシステムライフサイクルにおけるハードウェア設定、アプリケーションのソース・実行ファイル等の版管理を行うことにより、これらの変更を管理する。

機能要件		
1	加点	バグトラッキングツールと連携により、システムで使用している構成品目(CI)の構成情報の変更理由、変更内容及び変更を行った利用者に関する情報をすべて記録できること。
2	基本	システム全体の版管理が一元的にできること。
3	基本	複数の作業者が並行して、変更を反映させることができること。また、並行開発の結果生じる任意のリビジョン間の差分をマージできる機能を有すること。
4	基本	認証機能を実装しており、無権限者の利用が排除できること。
5	加点	保守ツールに含まれる統合開発環境(IDE)と連携して、チェックイン、チェックアウトができること。
6	加点	構成管理リポジトリ全体でリビジョン番号を管理することにより、各仕様変更でどのファイルがどのように変更されたのか確認が行えること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	ハードディスクの冗長化等により、可用性を高めたハードウェア構成を採用すること。
セキュリティ	基本	不正アクセスや情報漏えい、設定改ざん等、セキュリティ上のリスクに対応できる構成を採用すること。
パフォーマンス	加点	処理のピーク、最大同時利用者数等を想定して、事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	基本	対象とするシステムや保管するコンテンツの増加に伴い、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	すべての保管データのバックアップを取得できること。

関連する技術	
ソフトウェア構成管理プロセス	ソフトウェア構成管理プロセスは、必要に応じて過去の任意の状態を再現するため、ソフトウェア・ライフサイクル全体を通じて、ソフトウェア構成や構成アイテムの変化の記録を行う活動。 ISO/IEC TR 15846

・実務手引書に対応する項目：第 3 章 分離調達の実施手順 3.(2)③イ ソースコード変更履歴管理等(p 49)、第 4 章 分離調達プロジェクトの運営 4(3)ソースコード関係(p 66)

5.5.5.テスト環境(受け入れ環境)の機能要件／非機能要件

テスト環境(受け入れ環境)は、開発受託会社の開発環境で作成されたアプリケーションをビルドし、結合テスト、総合テストを実施するための環境である。

機能要件		
1	基本	開発環境で生成されたプログラムソースのビルドを行うことができること。
2	基本	結合テスト、総合テスト、ソフトウェア適格性確認テストを実施できる機能を有すること。
3	基本	AP サーバの複数インスタンス起動や仮想環境の活用により、一つの物理テスト環境(受け入れ環境)内に複数環境を保持する機能を有すること。
4	基本	認証機能を実装しており、無権限者の利用が排除できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	ハードディスクの冗長化等により、可用性を高めたハードウェア構成を採用すること。
セキュリティ	基本	不正アクセスや情報漏えい、設定改ざん等、セキュリティ上のリスクに対応できる構成を採用すること。
パフォーマンス	加点	処理のピーク、最大同時利用者数等を想定して、事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	基本	対象とするシステムや保管するコンテンツの増加に伴い、処理能力の柔軟な増強ができる構成とすること。
バックアップ	加点	すべての保管データ、環境のバックアップを取得できること。

5.5.6.テストツールの機能要件／非機能要件

テストツールは、各テストにおいてテスト作業の省力化を行うためのテストツール、テスト作業の自動実行やテスト結果のデータベース化を行うテスト管理ツールから構成される。

機能要件		
1	加点	テストスクリプト(テストケース)や各テストツールを自動実行し、テストの自動化を行う機能を有すること。
2	加点	構成管理ツールとの連携により、テストケースを成果物と一緒に管理する機能を有すること。
3	加点	要件(仕様)、テストケース、テストスクリプト、テスト結果等のテスト情報を一元的に管理する機能を有すること。
4	加点	テスト自動化ツールから出力されるテストデータを自動的に収集し、集計・分析する機能を有すること。
5	加点	単体テストや機能テストのテストツールは統合開発環境(IDE)に組み込んで使用ができること。
6	加点	負荷テストのテストツールはロードバランシング等の負荷分散機能への対応ができるよう、複数のサーバによる大量トランザクションの発生が可能で、複数の被テストサーバの処理結果を制御用端末に集約する機能を有すること。
7	加点	リグレッションテストを実施する機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	ハードディスクの冗長化等により、可用性を高めたハードウェア構成を採用すること。
セキュリティ	加点	不正アクセスや情報漏えい、設定改ざん等、セキュリティ上のリスクに対応できる構成を採用すること。
パフォーマンス	加点	テストチーム数、最大同時利用者数等を想定して、事前に性能要件を明確にし、十分な処理能力をもった構成とすること。また、パフォーマンステストを実施する場合は運用環境と同等の性能・機能をもったハードウェア・ソフトウェア構成とすること。
拡張性	加点	テストツールの追加、バージョンアップに伴い、処理能力の柔軟な増強ができる構成とすること。
バックアップ	加点	テスト環境、テストデータのバックアップを取得できること。

5.5.7.ステージング環境の機能要件／非機能要件

ステージング環境は、セキュリティレベル改善のために実施される OS やソフトウェア等のパッチ適用の影響による不具合の有無を検証するために使用される。なお、政府機関統一基準は、運用環境へのパッチ適用前にステージング環境等の評価用環境で事前評価を行うことを推奨している。

機能要件		
1	加点	運用(本番)環境と同等のハードウェア、ソフトウェアを有し、同等の機能・性能を有していること。
2	加点	運用環境と同等のハードウェアを用意できない場合は、仮想化ソフトウェアにより実現された仮想環境のサーバ、ストレージ上にステージング環境を構築できること。また、仮想環境上のステージング環境には運用環境と同等のソフトウェアを配置され、同等の機能を満たすことができること。
3	加点	ステージング環境を教育訓練に活用することにより、システム利用者が運用(本番)環境で実施できない更新処理を伴うユーザ教育を実施できる機能を有していること。
4	加点	仮想環境を用いずにステージング環境を構築する場合は、運用(本番)環境と同レベルのデータ量、負荷を使って、性能テスト、負荷テスト等を実施できる機能を有していること。
5	基本	ステージング環境は運用(本番)環境とは別の物理環境、もしくは運用(本番)環境とは別の物理環境上の仮想環境に構成され、運用環境へのパッチ適用前に必要となる事前評価や運用環境のトラブル再現試験等を実施できる環境であること。
6	基本	認証機能を実装しており、無権限者の利用が排除できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化、ハードディスクの冗長化等により、可用性を高めたハードウェア構成を採用すること。
セキュリティ	基本	不正アクセスや情報漏えい、設定改ざん等、セキュリティ上のリスクに対応できる構成を採用すること。
パフォーマンス	加点	運用環境向けの最終テスト環境として、事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	運用環境の機能強化、バージョンアップに伴い、処理能力の柔軟な増強ができる構成とすること。
バックアップ	加点	ステージング環境全体のバックアップを取得できること。また、仮想環境(仮想サーバ)利用時は、仮想サーバごとのバックアップも取得できること。

5.5.8.開発系 LAN、テスト系 LAN、系間 LAN(ブリッジ LAN)の機能要件／非機能要件

開発系 LAN、テスト系 LAN は、保守環境専用の構内ネットワーク(LAN)である。また、系間 LAN(ブリッジ LAN)、開発系 LAN・テスト系 LAN－運用(本番)系 LAN の間を接続するためのネットワークである。政府機関統一基準は、保守環境と運用環境の明確なネットワークの分離を求めている。

機能要件		
1	基本	開発系 LAN・テスト系 LAN は物理的なネットワーク分離、VLAN 等の活用により、運用(本番)系 LAN と切り離されていること。
2	加点	開発系 LAN・テスト系 LANー運用(本番)系 LAN 間はスイッチ、ルータ等の通信機器が配置され、許可された端末、サーバ間以外の通信は行えないこと。
3	加点	開発系 LAN、テスト系 LAN、系間 LAN(ブリッジ LAN)は内部専用ネットワークとし、インターネット等の外部ネットワークと接続されていないこと。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	必要に応じて、ネットワーク機器の冗長化を行えること。
セキュリティ	基本	ルータ、スイッチ等の IP フィルタリング機能等により、保守環境と運用(本番)環境の通信が制御されること。
パフォーマンス	加点	保守環境のテスト環境として、事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	基本	保守環境の機能強化、バージョンアップに伴い、処理能力の柔軟な増強ができる構成とすること。

関連する技術
5.15 WAN, 省内 LAN, DNS/DHCP/Proxy の「関連する技術」を参照のこと。

5.5.9.監査プロセス

監査プロセスは、情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを検証・評価するプロセスである。監査業務は内部監査部門による内部監査のほか、外部組織等による第三者監査により実施される。

機能要件		
1	加点	運用環境、開発環境、テスト環境は、経済産業省が規定する「システム監査基準」に準拠した内部監査及び外部監査(第三者監査)を定期的に実施すること。
2	加点	監査人の助言、指摘に対して、適切な処置が実施されていること。
3	加点	監査においては、経済産業省「システム監査基準」(平成 16 年 10 月 8 日改訂)、「システム管理基準」(平成 16 年 10 月 8 日策定)、「情報セキュリティ管理基準」(平成 15 年 3 月 26 日策定)及び同運用規定を活用すること。
4	基本	事業目標の実現に向けて、情報戦略及び情報システムについて効果的かつ効率的に点検・評価するためにシステム監査の中長期計画書を策定すること。 また、システム監査の中長期計画書は府省個別組織の情報システム責任者の承認を得ること。
5	基本	中長期計画書を受けて、システム監査の基本計画書が年度単位で策定すること。また、システム監査の基本計画書は府省個別組織の情報システム責任者の承認を得ること。
6	基本	中長期計画書及び基本計画書に基づき、システム監査の個別計画書を作成すること。また、システム監査の個別計画書は府省個別組織の情報システム責任者の承認を得ること。
7	加点	必要に応じて、府省外の専門家に監査の一部を請け負わせること。
8	基本	個別の監査実施計画に従って監査をすること。
9	基本	当該システムの設計・開発・運用・保守が、信頼性、安全性、効率性の観点から適切に実施されていることを確認すること。

非機能要件（個別の要件がある場合のみ記述）		
独立性	基本	監査人は被監査主体と身分上、密接な利害関係を有していないこと。
専門性	基本	監査人は監査に関する適切な教育と実務経験を有しており、監査に関する知識、技能を保有していること。
権限・責任	基本	監査人の権限と責任は文書化された規定、又は契約書等により明確に定められていること。

関連する技術	
IT 内部統制フレームワーク	IT 内部統制フレームワークは違法行為や不正、ミスやエラー等なく、組織の基準・手続きに基づき業務が行われている事実を、IT を利用して管理・監視・保証をするための仕組み。 ISO/IEC 38500:2008、COBIT(R)4.1

COBIT(R)は情報システムコントロール協会(Information System Audit and Control Association: ISACA) / IT ガバナンス協会(IT Governance Institute: ITGI)の登録商標(trademark)である。COBIT(R)の内容に関する記述は、ITGI(R)に著作権がある。

5.6.サーバ

5.6.1.定義

　サーバとは、共通基盤等の機能やデータ、サービスを提供するコンピュータである。
　サーバは、省内 LAN/WAN に接続された端末や個別業務システムからの要求を処理し応答を返す役割を担い、サーバハードウェアやサーバ間通信をつかさどるネットワークとその構成には、高い信頼性、可用性、保守性が求められる。
　サーバには提供する機能やサービスによって異なる役割(Web サーバ、DB サーバ、AP サーバ等)があり、それらが適切に配置・構成される必要がある。特に、安定したサービス提供、将来の負荷増大への対応としてサーバ特性に応じた拡張・増強方式が採用可能であることが重要になる。例えば、スケールアップ方式(サーバきょう体内の CPU 等の能力や数を増加させることで、性能向上を実現するサーバ実装方式)、又はスケールアウト方式(サーバきょう体を複数設置し、処理を並列に行うことで性能向上を実現するサーバ実装方式)による拡張・増強が可能な構成であることが求められる。
　また、サーバが提供する機能の配置・構成に関しては、仮想化ソフトウェアを利用することにより複数の機能やサービスを提供するサーバ群を 1 台のサーバハードウェア上に統合する構成が可能であることも求められる。仮想化ソフトウェアとは、一つのハードウェアで複数の仮想マシンを実行する機能を実現するソフトウェアで、ハードウェアのパフォーマンスの低下を最小限に抑えつつ、複数のオペレーティングシステムを一つのハードウェア上で同時に稼動させることが可能となる。それぞれのオペレーティングシステムには、仮想 CPU、ネットワークインタフェース、ストレージが割り当てられる。(図 5.6-2 参照)
　サーバは、5.7 ストレージと密接な連携をもちながら、高い信頼性、可用性、保守性を備えることにより、分散処理が可能となると同時に一元的に統合管理ができ、さらなる仮想化、集約、統合の実現が期待される。
　なお、本節では、主にサーバ室に設置されるサーバとサーバファームアクセス層のネットワーク(サーバ LAN)について記述する。省内 LAN/WAN 等のコア・エッジアクセス層及びネットワーク関連機器全体の記述については、5.15 を参照のこと。

サーバの機能・サービス	
機能・サービス	定義
サーバハードウェア	共通基盤が提供する機能やサービスの情報処理を行うコンピュータのハードウェア。オペレーティングシステム・ミドルウェア・アプリケーションの種類、処理する情報量の変化をかんがみ、それらが稼動することのできる機能や構成を有し、効率性、信頼性、可用性、柔軟性、そして高い保守性を備えていることが求められる。
サーバ LAN	共通基盤内のサーバ間の通信を行うための LAN 及びネットワーク機器。
Web サーバ	共通基盤においてポータルサイト等の Web ベースの情報の配信サービスを担当するソフトウェア及びそれを実行するハードウェア構成。配信するべき HTML 文書や画像等のデータを保存し、Web ブラウザ等からの要求に応じて、これらのデータを抽出・整形して要求元に転送するためのサービスを提供する。
DB サーバ	共通基盤が提供する機能・サービス群が扱うマスターデータや取引データを格納・抽出して応答するサービスを提供するプログラム及びそれを実行するハード

	ウェア構成。クエリ言語によって記述された問い合わせを高速に処理できる機能を有する。DB サーバ上の情報は共通基盤が提供するサービスや機能からのクエリ要求に応じることができ、また要求に対する性能要件(レスポンスタイム、スループット、容量)を満たす必要がある。
AP サーバ	共通基盤が提供するサービスの中のビジネスロジック部分の実行・管理を提供するプログラム群及びそれを実行するハードウェア構成。共通基盤が提供する Web サービスのインタフェースの提供、ビジネスロジックのプログラムの実行、トランザクション管理、データベースへの接続等を行う。

5.6.2.概念図

基盤構成モデルにおける、各機能・サービス(サーバハードウェア、サーバ LAN、Web サーバ、DB サーバ、AP サーバ)の配置を示す。

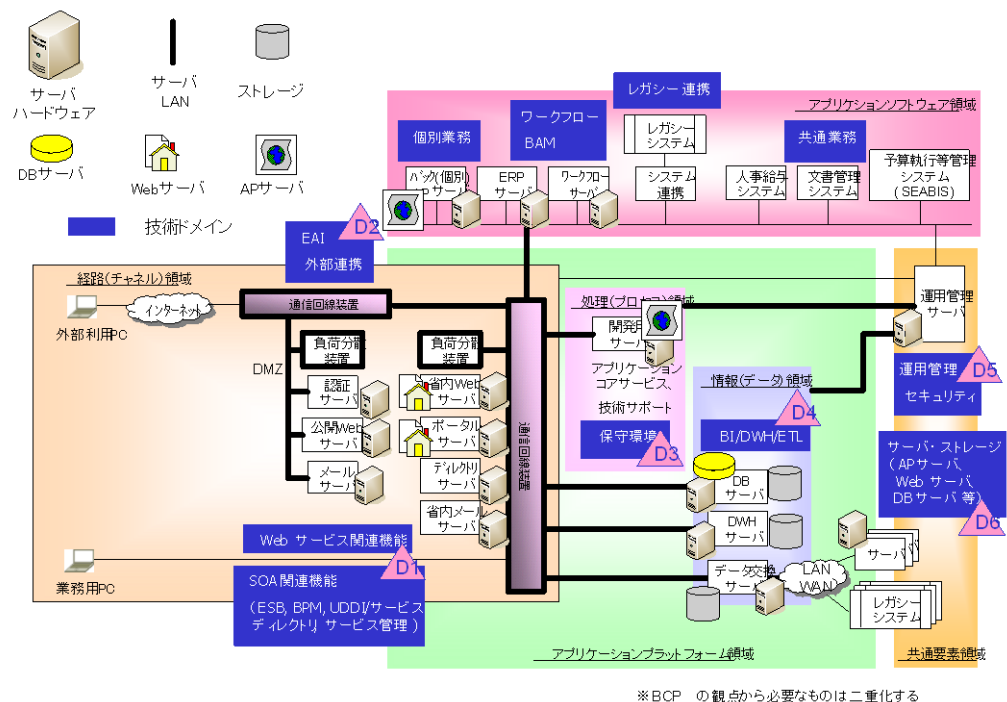



図 5.6-1 基盤構成モデルにおける「サーバ」の各種サービス・機能の配置

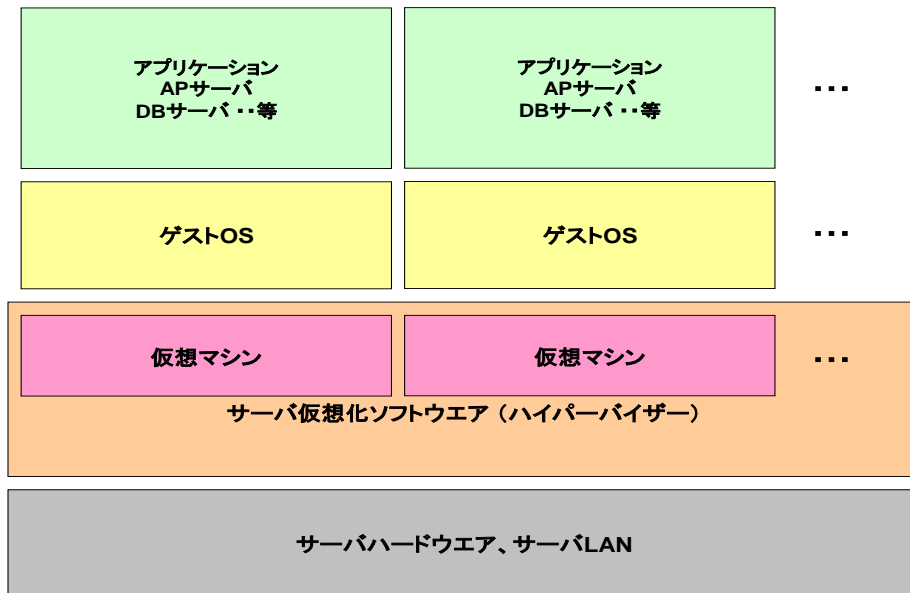



図 5.6-2 サーバ仮想化ソフトウェアによるサーバ環境の仮想化

5.6.3.サーバハードウェア

機能要件		
1	基本	サーバ上で稼動するアプリケーションプログラムの実行基盤及びアプリケーションプログラムと実行基盤とのインタフェースを提供する機能を有するオペレーティングシステム【Linux、Windows、商用 UNIX 等】が稼動すること。
2	基本	内蔵又は外部のディスクドライブからオペレーティングシステム【Linux、Windows 及び商用 UNIX 等】の起動(ブート)が行える機能を有すること。
3	基本	ネットワーク装置インタフェース【Ethernet(IEEE 802.3)、RS-232C 等】、そして周辺機器の接続が必要な場合には、【SerialATA、PCI、SCSI2、SCSI3、iSCSI、SAS、Infiniband、FibreChannel 等】のインタフェースを有すること。
4	加点	障害管理(予防検出を含む)を行うための情報が収集され、提供できること。 具体的には、【e-mail で故障箇所の情報を送る機能、SNMP で故障をトラップ通知する等】を有すること。
5	加点	サーバ内の構成情報や状態のデータを標準インタフェース仕様【SNMP、CIM 等】を介してモニタリングできること。遠隔地にある統合管理システムあるいはツールに対して通知し、逆に遠隔地からの構成変更の要求を受ける等の遠隔管理機能を有すること。
6	基本	サーバハードウェア上で稼動するオペレーティングシステムは、アプリケーションプログラムに対して API(Application Program Interface)を通してそのサービスと機能を提供できること。また、オペレーティングシステムのサービスと機能及び API の仕様は、標準化され広く普及している規格に準拠したものであること。
7	基本	サーバハードウェア上で稼動するオペレーティングシステムは、標準化されて広く普及している規格に準拠しているか、広く普及している CUI(Character-based User Interface)ベースのコマンドユーティリティ機能を提供していること。
8	基本	オペレーティングシステム上で稼動する、すべての機器を制御するプログラム(デバイスドライバプログラム)が存在すること。

非機能要件（個別の要件がある場合のみ記述）		
配置スペース(きょう体)	基本	サーバきょう体はプロセッサ(CPU)、メモリ、メインボード、内蔵ディスクドライブ(内蔵ディスクドライブを必要しないサーバの場合は必須ではない)、周辺機器インタフェース、電源等を含むものとする。 ・サーバきょう体の形態は、【ラックマウント、ブレード、タワー　等】であること。 ・ラックマウントの場合には、1台あたりEIA(米国電子工業会)規格に準拠する19インチサーバラック{4U以内}に収まること。 ・サーバきょう体がブレードの場合には、EIA規格に準拠する19インチサーバラック{7Uに6ブレード}に収まること。 ・それ以外の形状である場合には床設置面積及び形状が{幅 190cm×奥行き200cm×高さ220cm}、単位面積あたりの最大荷重が{100kg ／㎡以内}であること。 注意：一般的なオフィスでの耐荷重は100kg/㎡程度であるが、データセンターでは耐荷重 1000kg/㎡以上も一般的であり、データセンターに設置・収容する場合には 1000kg/㎡以上のサーバ製品を調達することもありうる。従って、本要件項目は、特に{例示}の採用について十分に留意し、サーバを設置・収容する予定施設に応じて{例示}を変更すること。予定施設が未定の場合には、前述のオフィスとデータセンターの耐荷重を参考とすること。
プロセッサ処理能力	基本	業務要件を満たす能力を有すること。又はプロセッサの処理能力が{64bit稼動周波数2GHz、4コア}以上であること。又は、 ・{SPECint 2006 base}値が{30}相当以上であること。 ・{SPECweb 2005 base}値が{5,000}相当以上であること。 ・{SPECfp 2006 base}値が{30}相当以上であること。
プロセッサ命令セットアーキテクチャ	基本	実行命令アーキテクチャが公開され、第三者によるアプリケーション開発が可能であるプロセッサであること。【x86、x64、IA64、POWER、SPARC 等】
プロセッサの拡張性	加点	将来想定される処理能力増大の要求に応じてプロセッサの数もしくは性能を拡張することが可能であること。ただし稼動ソフトウェアがスケールアウトによる処理能力増大が可能な仕様である場合には、サーバへのプロセッサ拡張性は必要ではない。
バックアップ	基本	オペレーティングシステム単位で内蔵又は外部ディスクドライブに格納されているシステム及びデータバックアップが可能な構成を有すること。
メモリ容量	基本	業務要件を満たすため、又はデータ処理を行うために十分なメモリを搭載していること。搭載メモリ容量が{4GB}以上であること。又はプロセッサコアあたり{4GB}以上のメモリが搭載できること。
メモリ拡張性	基本	処理に必要なデータ容量に応じてメモリ量を増設できること。最大{16GB}以上まで増設可能であること。ただし稼動ソフトウェアがスケールアウトによる処理能力増大が可能な仕様である場合には、サーバのメモリ拡張性は必要ではない。
メモリ可用性	基本	シングルビットエラー発生時にオペレーティングシステムに依存せず、ハードウェアで処理を止めることなく、自動的に誤りデータを補正して処理を継続できること。
	加点	マルチビットエラー発生時にオペレーティングシステムに依存せず、ハードウェアで処理を止めることなく、自動的に誤りデータを補正して処理を継続できること。
I/F 転送能力の拡張	加点	要求されるデータ転送能力が満たされない場合には、複数 I/F カードの集

性		束等の手段でデータ転送能力を拡張する機能を有すること。ただし稼動ソフトウェアがスケールアウトによる処理能力増大が可能な仕様である場合には、サーバのI/F 転送能力の拡張性は必要ではない。
I/F 可用性	加点	単一の I/O インタフェースが故障等で障害が発生した場合であっても、ほかの同一種類の正常なI/O インタフェースによって自動的に処理が続行できること。
I/F 保守性	加点	障害が発生したインタフェースをシステム稼動中に交換できること。もしくはクラスタ化等の手段を用いて、当該システムのサービスを停止させずインタフェースの交換ができること。
内蔵及び外部ディスクドライブの容量	基本	ディスク領域容量が{100GB 以上}であること。容量は「物理容量」とする。
内蔵及び外部ディスクドライブの可用性	基本	複数の【ディスクドライブ,SSD 等】を束ねて単一のデバイスとして動作させることができ単一ディスクの故障時にもデータ消失や業務停止等が発生しないこと。
	加点	サーバを停止させずにディスクドライブの交換が行えること。
ディスク領域の拡張性	基本	ディスク領域容量を最大{200GB}まで増設できること。
電源装置の容量	基本	サーバを稼動させ続けるために必要な電源容量を供給できること。
電源装置の保守性	加点	サーバを停止させずに電源の交換ができること。
電源装置の可用性	加点	冗長構成により単一の電源の故障が発生しても、正常なほかの電源にて必要な電力の供給が可能なこと。
電源供給の可用性	加点	・無停電電源装置(UPS)等を利用して、入力電源に停電等の異常が発生しても、{5 分以上}はサーバを稼動できること。 ・{5 分}を超えて異常が継続した場合は、自動でシステムを正常終了させる機能を有すること。
電源供給系列の多重化	加点	2 系統からの電源供給を受け、設備の点検/工事等に際してもサーバを稼動し続けるための電源を供給できること。
無停電電源装置(UPS)の耐障害性	加点	UPS の故障時にも、UPS 回路をバイパスして、サーバへの電源供給を継続する機能があるか、又は 2 系統受電にて同等の回避策がとれること。また、故障したことをシステム管理者に通知する機能を有すること。
無停電電源装置(UPS)バッテリーの保守容易性	加点	・稼動中に自己診断を行い、異常の際は、管理者に通知する機能があること。 ・規定の運用が行えなくなる以前に、バッテリーの交換を促すメッセージをシステム管理者に通知できること。 ・バッテリーの検査は{2 週間}以内ごとに自動実施されること。 ・バッテリー異常通知を SNMP トラップで通知できること。
HW モジュール冗長性	加点	単一又は、複数のサーバハードウェアきょう体の組み合わせによって、これらを構成する主要なハードウェア部材【CPU、メモリ、ハードディスク、電源、FAN 等】が冗長化され、一つの部材の障害が発生しても業務が継続できること。ただし、ソフトウェアの機能により必要な冗長性が確保できる場合はこの限りではない。
調達リードタイム	基本	サーバを増設又は新設するために必要な所要時間(調達リードタイム)が原則{8 週間}以内であること。
HW 部材の増設作業の保守性	加点	サーバを構成するハードウェア資源、具体的には【プロセッサ、メモリ、物理ディスクドライブ、周辺装置インタフェースボード 等】の増設を、サーバを停止せずに行えること。もしくはクラスタ化等の手段を用いて、当該システムのサービスを停止させずにハードウェア資源の増設を行うシステム構成が可能なこと。

OS/ミドルウェア保守性	加点	以下の保守性を有すること。 ・セキュリティパッチを適用する際の当該システムのサービス停止時間が{2 時間}以内であること。 ・保守・サポート期間の残存期間が{5}年以上であること。 ・修正パッチを適用する際の当該システムのサービス停止時間が{2 時間}以内であること。 ・ただし、セキュリティパッチあるいは修正パッチを適用する際の当該システムのサービス停止時間が{2 時間}以上の場合には、クラスタ化等によりサーバが冗長化されたシステム内で、業務を待機サーバへ切り替える等の運用を行い、業務の停止時間を{2 時間}以内にできること。
HW 保守期間	基本	構成するハードウェアの故障時のサポート期間(保守期間)が{5}年以上であること。
グリーン調達(グリーンIT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「電子計算機」に対して規定されている基本方針に適合した製品)であること。
国際エネルギースター(グリーン IT)	加点	国際エネルギースタープログラムに対応すること。

関連する技術	
監視・制御プロトコル/ サーバ管理標準インタフェース仕様	SNMP(Simple Network Management Protocol) CIM(Common Interface Model)
ネットワークインタフェース、周辺機器インタフェース	SerialATA、PCI、RS-232C、Ethernet(IEEE 802.3)、 Fiber Channel、SCSI2、SCSI3、iSCSI、SAS、FC-AL、FC-SW、Infiniband
EIA	EIA(米国電子工業会)
「環境物品等の調達の推進に関する基本方針」	http://www.env.go.jp/policy/hozen/green/g-law/archive/bp/h19bp.pdf
SPEC	SPEC(Standard Performance Evaluation Corporation) SPECint、SPECfp
カーネル API 標準	POSIX API 標準(ISO/IEC 9945-1) Linux Standard Base
オペレーティングシステム コマンド/ユーティリティ標準	POSIX コマンド標準(ISO/IEC 9945-2:1993 Information technology、IEEE Std 1003.2)
バッテリー異常通知規定/UPS 異常通知規定	JEMA(社団法人日本電機工業会) 参考 http://www.jema-net.or.jp/Japanese/standard/ups/
電子計算機の性能の向上に関する製造事業者等の判断の基準等	電子計算機の性能の向上に関する製造事業者等の判断の基準等 平成 11 年 3 月 31 日 通商産業省告示第 194 号 最終(全部)改正 平成 18 年 3 月 29 日経済産業省告示第 50 号

5.6.4.サーバ LAN

機能要件		
1	基本	TCP/IP プロトコルを介した通信を行えること。
2	基本	データリンク層/ネットワーク層のパケットスイッチング機能を有すること。
3	加点	ネットワーク装置は管理インタフェース機能を有すること。
4	加点	帯域制御の設定及び変更等を行うトラフィック制御機能を有すること。
5	基本	ファイアウォール機能を備え、当該装置に接続する回線の最大実効性能が{1Gbps}以上、最大パケット処理数が{2Mpps}以上であること。
6	基本	不正アクセスを検出し、検出した不正アクセスを遮断するための侵入検知及び防止機能を備え、かつその最大回線接続帯域が{1Gbps}以上であること。
7	基本	改ざん検知の機能を備え、その性能値すなわち検知装置のパケット処理能力が{2Mpps}以上であること。
8	基本	ウイルス検知機能を有し、その性能値すなわち検知装置のパケット処理能力が{2Mpps}以上であること。
9	基本	負荷分散装置を複数台設置し、冗長構成を作れること。また、負荷分散装置の故障に対し、あらかじめ設定したもう1台の負荷分散装置が、他方の負荷分散装置が保持していたセッションを引き継ぎ、ユーザのアクセスを継続させる機能を有すること。
10	基本	物理的な接続形態とは独立した、データリンク層での仮想的なグループ設定を行う VLAN 機能を有すること。VLAN 機能は、{16}個以上設定できること。

非機能要件(個別の要件がある場合のみ記述)		
帯域容量	基本	回線速度が{理論値で 1Gbps}以上を提供できるネットワークであること。
ルータ・スイッチの可用性	加点	ルータ・スイッチ内部が完全に二重化されている、又は装置の冗長化がなされていること。
ルータの保守性	加点	ルータにおける、ルーティング情報やファームウェアの更新は最大{5 分}以内で完了するか、冗長化された装置へネットワークを切り替え、業務に影響を与えずに実施できること。
ルータ・スイッチの運用管理容易性	基本	ルータ・スイッチはネットワーク経由でのマネジメント機能をもち、異常発生時のポートの停止や、ルーティング情報の書換え等を保守用の別ネットワーク経由でできること。
最大停止時間	加点	共通基盤内 LAN の稼動停止時間=利用負荷時間の月次最大値が{1 時間}以内であること。
平均応答時間	基本	ノード(通信機器及びサーバ)間の往復遅延時間の月間平均値が{100msec}以下であること。なお、ネットワークの使用率は{30%}を超えないことを前提としてよい。
ルーティング機能の可用性	加点	データリンク層/ネットワーク層の経路の冗長化機能を有すること。
可用性(LAN 多重化)	加点	LAN が冗長化されていること。

関連する技術	
通信プロトコル	TCP/IP
LAN 規格	Ethernet
仮想 LAN(VLAN)	IEEE 802.1Q
監視・制御プロトコル	SNMP(Simple Network Management Protocol)
グリーン調達(グリーン IT)	「環境物品等の調達の推進に関する基本方針」 http://www.jkiss.or.jp/green/siryo2.pdf

5.6.5.Web サーバ

機能要件		
1	基本	Web ブラウザ等のクライアント PC からの要求に対して、Web サーバ上に格納されたコンテンツをHTTP もしくはそれに準ずるプロトコルにより返送できること。加えてプログラムを実行することによって動的に HTML データを作成して返送する機能を有すること。
2	基本	ログイン状態や画面遷移を管理することのできるセッション管理機能を有すること。
3	基本	IP 認証やユーザ認証等により、Web サイトに対する認証と認可(承認)が行えること。またサーバ外部のディレクトリサービスと連携した認証・認可を行えること。
4	加点	アクセスログ記録：アクセス元 IP アドレスと日付・時刻、アクセスされたファイル名、リンク先ページ、アクセスしたユーザの Web ブラウザ名称や OS 名称、処理にかかった時間、受信バイト数、送信バイト数、サービス状態コード等の情報をログとして記録できること。
5	加点	監査イベント通知：認証拒否又は権限を越えたアクセスの事象についてはその情報をリアルタイムに管理ツール等に通知できること。
6	加点	監査レポート出力：ログの情報のサマリーを報告書の形式で閲覧できること。報告書の形式で閲覧できること。
7	基本	SSL や TLS 等のプロトコルを使用して WWW の通信データを暗号化できること。 (データ盗聴・改ざん・なりすましを防御することができること)
8	加点	Web サーバの提供しているサービス・機能が正常に稼動していることを監視し、性能劣化や障害を検出した場合には障害イベントを統合管理ツールに障害の事象を通知するとともに、障害の種類や原因を特定するために必要な情報を保存する機能を有すること。
9	加点	複数の Web サーバの各種設定を遠隔地 PC から管理することが可能であること。
10	基本	ネットワークを介してサーバに送られる処理要求を一括して受け、管理し、複数のサーバ群に分散して中継・送信する負荷分散処理機能を有すること。
11	基本	負荷分散装置の分散方式は、ラウンドロビンと、応答時間を考慮した負荷分散とが選択できること。また、どちらの方式の場合でも、事前に設定したレスポンス時間以上応答がないサーバに対して負荷分散処理をやめる機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
処理能力	基本	要求サービスレベル及び利用ピーク想定に基づいた、十分な処理能力(1 秒あたりの平均リクエスト処理能力)を有すること。
サーバ拡張性	基本	負荷を分散させるために複数のサーバハードウェア上で処理を多重化して処理効率を高められること。
サーバ保守性	基本	Web サーバの増設・拡張作業を、業務停止させることなく行えること。
可用性	基本	Web サーバソフトウェアを複数のサーバハードウェア上で稼動させ、単一のサーバハードウェアで障害が発生しても、正常なサーバハードウェアが後続の処理要求を受けることができること。
サービス時間帯	基本	Web サーバのサービスを下記の時間帯で提供できること。 {平日 8:00−22:00}

関連する技術	
マークアップ言語	HTML
ディレクトリサービス	LDAP
動的 Web ページ生成技術	JSP(Java Server Pages) Java Servlet ASP.NET

5.6.6.DB サーバ

機能要件		
1	基本	リレーショナルなデータ表現形式のデータベースを管理するシステム(リレーショナルデータベース管理システム)、又は、XML データを取り扱うことのできる XML データベースシステムであること。
2	基本	問い合わせ言語(データ定義言語:DDL、データ操作言語:DML、データ制御言語:DCL)を使って記述したプログラムを実行することにより、データベースの定義、データのアクセス、アクセス制御を行えること。
3	基本	トランザクション処理機能を有すること。
4	基本	認証・認可:データベースにアクセスする利用者を、識別子を通して特定し、許可されている利用者ならばアクセスを許可し、それ以外は拒否する機能を有すること。 ユーザの役割ごとに、データベース上のオブジェクト(テーブル、ビュー、列)ごとに行うことのできるアクションを限定できること。
5	基本	データベースにて維持・管理するデータの暗号化及び復号を行えること。その際の暗号化方式を選択できること。
6	基本	監査:データベースの監査を行える機能を有すること。利用者が実行した SQL 文の実行履歴をログの形式で記録できること。また権限を越えたアクセスの事象についてはその情報を管理ツール等に通知できること。またログの情報をサマリーとして取りまとめた報告書の形式(レポート形式)で閲覧できること。
7	基本	性能管理:DB サーバの構成要素の性能(トランザクション処理スループット、レスポンスタイム等)を監視し、サービスが適切に提供されていることを監視する機能を有すること。性能の劣化の兆候を検出した場合には、自動又は手動で性能を最適化することができること。

非機能要件 (個別の要件がある場合のみ記述)		
可用性	基本	DB サーバを以下の一つ又はいずれかの方式を組み合わせたシステム上で稼動させ、障害が発生しても、異常を自動的に検出して最長{10 分}以内に DB へのアクセスを再開できる構成を有すること。 ・フォールトトレラント ・ホットスタンバイ ・クラスタリング ・ミラーリング
処理能力	基本	データベース性能値(例えばスループットやレスポンスタイム等)の要求にこたえる十分な処理能力を有すること。
データ容量	基本	共通基盤で取り扱うデータ量{2TB}を格納するのに十分な容量をもつこと。
処理能力拡張性	基本	複数のサーバで処理を多重化して負荷を分散させる、又はデータベースサーバ内の計算リソースを拡充する等でデータベースアクセスの処理効率を高められること。
データベース耐障害性	基本	データベース上のデータの破損等の障害が発生した場合に、データベースシステム及び取り扱いデータを復旧する手段を有すること。
バックアップ	基本	オンライン・バックアップが採取できること。
	基本	テーブル単位・データベース単位で差分・全体のバックアップを採取できること。
	加点	記憶媒体(デバイス)単位でバックアップを採取できること。
サービス時間帯	基本	データベース機能を下記の時間帯で提供できること。 {平日 8:00-22:00}

関連する技術	
DB 問い合わせ言語	SQL92 SQL99 SQL2003 XQuery Xpath
ディレクトリサービス	LDAP
データ暗号化技術	DES AES RC4

5.6.7.AP サーバ

機能要件		
1	基本	Web サービス：SOAP や WSDL 等の Web サービス技術を利用したサービスを提供できること。
2	基本	Java コンポーネント、.NET コンポーネント等のコンポーネントアプリケーションを構築・実行するための基盤を有すること。
3	基本	AP サーバ上で実行されるアプリケーションプログラムが DB サーバ上のデータベースに接続してデータのアクセスを行うためのインタフェースと機能を有すること。
4	基本	分散トランザクション：複数のデータベース/サーバにまたがるデータの更新を単一のトランザクションとして処理できること。
5	基本	分散オブジェクト：遠隔地のサーバ間でプログラム同士がメッセージ通信を行うことのできる機能を有すること。
6	基本	セキュリティ機能：以下の脅威からAPサーバ及びアプリケーションを防御するための機能を有すること。 ・ネットワーク盗聴(Web サーバと AP サーバ間、AP サーバと DB サーバ間) ・不正アクセス なお、防御のための機能は、AP サーバ単独の機能として実現していなくとも、ネットワーク機器等の機能を用いてシステム全体の構成として実現できていればよい。ネットワーク盗聴防止は通信の暗号化を必ず求めるものではなく、AP 通信パケットが Web サーバと AP サーバ間、AP サーバと DB サーバ間以外に流れなければよい。不正アクセス対策は IP アドレス制限等の設定により、AP アクセスを Web サーバからのアクセスだけに制限できればよい。
7	基本	性能管理：DB サーバの構成要素の性能(トランザクション処理スループット、レスポンスタイム等)を監視し、サービスが適切に提供されていることを監視する機能を有すること。性能の劣化の兆候を検出した場合には、自動又は手動で性能を最適化することができること。
8	基本	アプリケーションプログラム群、サービス群を AP サーバ上に配信・配布して利用/提供可能な状態にできること。
9	基本	AP サーバへの処理要求に対する認証と認可(承認)が行えること。その際に AP サーバ外部のディレクトリサービスと連携した認証・認可が行えること。

非機能要件（個別の要件がある場合のみ記述）		
処理能力	基本	{1 秒あたりの平均トランザクション処理能力}が{30 件}以上であること。
サーバ多重化(負荷分散)機能	基本	複数のサーバで処理を多重化して処理効率を高められること。
スレッド多重化(マルチスレッド)処理	基本	サーバ内で複数のスレッドを生成して実行することでトータルな処理効率を向上させることができること。

過負荷時のリクエストの信頼性	基本	AP サーバへの処理要求リクエスト量の増大(高負荷状態)に対して、AP サーバ内で処理待ちのリクエストの待ち行列(キュー)をもち、リクエストの損失を防ぐ機能を有すること。
サーバ拡張及び動的再構成	基本	AP サーバの拡張を行える構成を保有し、またシステムを停止させることなく拡張作業を動的に行えること。
AP サーバ可用性	基本	AP サーバが提供しているサービス・機能が性能劣化や障害がなく正常に稼動していることを監視(死活監視)し、障害を自動検出し、復旧を行うことができること。
サービス時間帯	基本	AP サーバのサービスを下記の時間帯で提供できること。 {平日 8:00-22:00}

関連する技術		
Web サービス関連技術	基本	SOAP WSDL
コンポーネントプログラム実行基盤技術	基本	J2EE .NET
データベースアクセス技術	基本	OLE DB ODBC JDBC ADO.NET
分散トランザクション技術	基本	Java Transaction API (JTA) COM+
ディレクトリサービス技術	基本	LDAP

5.6.8.仮想化への対応

1	基本	仮想化機構により実現された仮想化ゲストサーバなどから構成される仮想化環境において物理サーバ環境と同等のソフトウェアを配置でき、同等の機能を満たすことができること。

5.7.ストレージ

5.7.1.定義

ストレージとは、共通基盤内で取り扱うデータを格納するための外部記憶装置である。
共通基盤では、ハードディスク装置及びテープドライブ装置をストレージとして想定している。
ストレージは、省内LAN/WANに接続された端末や個別業務システムからの要求によりデータを格納する役割を担うため、高い信頼性、性能が求められる。

ストレージは 5.6 サーバと密接な連携をもちながら、高い信頼性、可用性、保守性を備えることにより、分散処理が可能となると同時に一元的に統合管理ができ、さらなる仮想化、集約、統合の実現が期待される。

ストレージの機能・サービス	
機能・サービス	定義
ディスクストレージ	主に共通基盤内にて取り扱うデータ、データベース、システムデータ等を格納しておくための外部記憶装置。ハードディスク装置を想定する。
テープストレージ	主に共通基盤内にて取り扱うデータ、データベース、システムデータ等を媒体にバックアップ/アーカイブ/マイグレーション/データ交換等を実施するための外部記憶装置。テープ装置もしくは仮想的なテープ装置を想定する。

5.7.2.ディスクストレージ

機能要件		
1	基本	オペレーティングシステム【Linux、Windows、商用 UNIX 等】の起動を行うことができること。
2	基本	複数のディスク装置を束ねて単一のデバイスとして動作させることができ単一ディスクの故障時にもデータ消失や業務停止等が発生しないこと。
3	加点	ディスク装置の複数同時故障にも対応可能であること。
4	基本	アレイ装置内に 1 台以上のスペアディスクが設定できること。
5	基本	【ファイバーチャネルスイッチ等】のゾーニング機能により、アクセス制御が可能であること。又はディスク装置の設定により、アクセス制御が可能であること。
6	基本	共用ストレージへのアクセス制御機能として、論理ユニット番号[LUN]による不要なサーバからのアクセス防御が可能であること。
7	加点	単一の電源装置の障害が発生してもサービス停止に至らない冗長構成及び電源容量を有すること。
8	基本	ストレージ装置は【TCP/IP,FC,FCIP,FCoE,SCSI、iSCSI,SAS,Infiniband 等】の I/O インタフェースを有すること。
9	基本	ストレージ内のディスクアクセス性能のチューニングや、構成の最適化及び拡張の作業を支援する機能を有すること。
10	加点	ストレージの機能、又は運用管理ツール等により、構成モジュール(物理ディスクドライブ、テープドライブ、電源、冷却ファン、I/O 制御装置及びインタフェース、キャッシュメモリ、I/O ポート等)の障害の検出と予防検出を行うための情報が収集され、適切に管理できる障害管理機能を実現できること。
11	基本	ストレージ内の構成情報や状態のデータを保有し、その情報を遠隔地にある統合管理システム及びツールに対して通知したり、逆に遠隔地からの構成変更の要求を受けたり等の遠隔管理機能を有すること。

12	加点	災害時等の遠隔地におけるデータ回復のために、遠隔地に整合性のあるデータを保管し、災害時には保管したデータを復元することで、業務や事業を再開できる機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
アレイ装置可用性	基本	ディスク装置が故障した場合でも RAID 技術等によりデータ・アクセスを継続して行うことができ、データ冗長性の自動復旧が可能であること。
アレイ装置保守性	加点	・無停止でディスク装置の交換及び増設が行えること。
論理ディスク・ボリュームの構成変更	加点	対応するオペレーティングシステムにおいては、システムを停止させずに、論理ディスク・ボリュームの構成変更、論理ディスク・ボリュームの追加・変更を行えること。
I/O インタフェースの可用性	加点	ストレージ装置のインタフェース【TCP/IP, FC, FCIP, FCoE, SCSI, iSCSI, SAS, Infiniband 等】は、冗長構成を有すること。
ストレージデータ帯域幅	基本	サーバとストレージ間の最大データ転送量が{100M バイト/秒}以上であること。
チャネル/ホストインタフェース拡張性	加点	要求されるデータ転送能力が満たされない場合に、同一種類のインタフェースを複数束ねることでデータ転送能力を増幅できる構成を有すること。
チャネル/ホストインタフェース転送能力	基本	I/O チャネル/ホストインタフェースのデータ転送能力が{100M バイト/秒}以上であること。
データ容量	基本	共通基盤で取り扱うデータ量{2TB}を格納するのに十分な容量をもつこと。
ユーザ割り当てデータ容量	基本	NAS,ファイルサーバ等で利用者に記憶領域を割り当てる場合には 1 ユーザに割り当てることのできる領域の容量の最大サイズが{1GB}以上であること。
サーバへのディスク容量割り当ての変更	基本	対応する OS が搭載されたサーバへのディスク容量の拡張を動的に実行可能であること。
バックアップ	加点	サーバと独立して、ストレージ装置自身がボリュームの複製を行う機能を有すること。
電源供給の可用性	加点	・無停電電源装置(UPS)等を利用して、入力電源に停電等の異常が発生しても、{5 分以上}はストレージを稼動できること。 ・{5 分}を超えて異常が継続した場合は、自動でストレージを正常終了させる機能を有すること。
電源供給系列の多重化	加点	2 系統からの電源供給を受け、設備の点検/工事等に際してもストレージを稼動し続けるための電源を供給できること。
無停電電源装置(UPS)の耐障害性	加点	UPS の故障時にも、UPS 回路をバイパスして、ストレージへの電源供給を継続する機能があるか、又は 2 系統受電にて同等の回避策がとれること。 また、故障したことをシステム管理者に通知する機能を有すること。
無停電電源装置バッテリーの保守容易性	加点	稼動中に自己診断を行い、異常の際は、管理者に通知する機能があること。 ・規定の運用が行えなくなる以前に、バッテリーの交換を促すメッセージをシステム管理者に通知できること。 ・バッテリーの検査は{2 週間}ごとに自動実施されること。 ・バッテリー異常通知を SNMP トラップで通知できること。
機器リードタイム	基本	ストレージを増設又は新設するために必要な所要時間(調達リードタイム)が原則{8 週間}以内であること。
HW 冗長性	加点	構成するハードウェア部材は、緊急停止スイッチ、バックボード、きょう体等を除き冗長化されていること。
システム性能値	基本	ストレージとしてのI/O 性能値が{SPC-1 ベンチマークで 10,000 以上}相当

		であること。
拡張データ容量	基本	装置導入の後、{5TB}まで、容量を拡張できること。
HW 保守期間	基本	構成するハードウェアの故障時のサポート期間(保守期間)が{5}年以上であること。
グリーン調達(グリーンIT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「磁気ディスク装置」に対して規定されている基本方針に適合した製品)であること。

関連する技術	
ディスク装置信頼性向上技術	RAID、Grid Storage
ストレージインタフェース	Fibre Channel (FC-AL、FC-SW)、 SCSI、LAN(iSCSI/NAS)、SAS、Infiniband
監視・制御プロトコル	SNMP(Simple Network Management Protocol)
「環境物品等の調達の推進に関する基本方針」	http://www.env.go.jp/policy/hozen/green/g-law/archive/bp/h19bp.pdf
バッテリー異常通知規定/UPS異常通知規定	JEMA(社団法人日本電機工業会) 参考 http://www.jema-net.or.jp/Japanese/standard/ups/
磁気ディスク装置の性能の向上に関する製造事業者等の判断の基準等	磁気ディスク装置の性能の向上に関する製造事業者等の判断の基準等 平成 11 年 3 月 31 日 通商産業省告示第 195 号 最終(改正)改正 平成 18 年 3 月 29 日経済産業省告示第 51 号

5.7.3.テープストレージ

機能要件		
1	加点	単一の電源装置の障害が発生してもサービス停止に至らない冗長構成及び電源容量を有すること。
2	基本	【SANFC、SCSI、SAS 等】の I/O インタフェースを有すること。
3	基本	ストレージの機能、又は運用管理ツール等により、構成モジュール【テープドライブ、電源、冷却ファン、I/O 制御装置及びインタフェース、キャッシュメモリ、I/O ポート 等】の障害の検出と予防検出を行うための情報が収集され、適切に管理できる障害管理機能を実現できること。
4	加点	データを保存する際、重複部分を自動的に検出・削除する機能を有すること。

非機能要件 (個別の要件がある場合のみ記述)		
テープストレージデータ帯域幅	基本	サーバとテープストレージ間の最大データ転送量が{80M バイト/秒}以上であること。
チャネル転送能力	基本	I/O チャネル/ホストインタフェースのデータ転送能力が{100M バイト/秒}以上であること。
機器リードタイム	基本	ストレージを増設又は新設するために必要な所要時間(調達リードタイム)が原則{8 週間}以内であること。
格納データ容量	基本	テープストレージに格納できるデータ容量の最大サイズが{10TB}以上であること。

関連する技術	
ストレージインタフェース	Fibre Channel (FC-AL、FC-SW)、 SCSI、LAN(iSCSI/NAS)、SAS、Infiniband
監視・制御プロトコル	SNMP(Simple Network Management Protocol)

5.7.4.仮想化への対応

1	基本	仮想化ソフトウェアにより実現された仮想化ストレージなどから構成される仮想化環境において物理サーバ環境と同等のソフトウェアを配置でき、同等の機能を満たすことができること。

5.8.共通 PC・オフィスプリンタ

5.8.1.定義

共通 PC・オフィスプリンタとは個人が情報システムへのアクセスや、文書作成等のオフィスワークに利用する端末のことである。本章では共通 PC で利用する操作環境等を提供するコンピュータ・ソフトウェアのことを共通オペレーション環境と定義する。共通PCには、単体で共通オペレーション環境を利用できるパーソナルコンピュータと、シンクライアントサーバ上で共通オペレーション環境を利用できるシンクライアントの 2 種類が存在する。以下に共通 PC・オフィスプリンタを定義する。

共通 PC・オフィスプリンタ	
項目	定義
パーソナルコンピュータ	単体で共通オペレーション環境を利用できる端末。
シンクライアント	シンクライアントサーバ等に接続する端末。
オフィスプリンタ装置	端末や情報システムからの指示に基づいて、情報を紙等に印刷するコンピュータ周辺機器。

シンクライアントサーバとは、共通オペレーション環境を提供し、ネットワークを経由しシンクライアントからの接続を受け付けるサーバのことと定義する。

5.8.2.共通 PC・オフィスプリンタの共通機能要件

共通 PC・オフィスプリンタにおける共通の機能要件を以下に示す。

共通 PC・オフィスプリンタの共通の機能要件		
1	基本	稼動している端末からネットワーク接続できること。 （本要件は庁内で使用するものに適用する。又は出張用は稼動しているという条件を外す。）

共通 PC・オフィスプリンタの共通の非機能要件		
ハードウェア保守期間	基本	構成するハードウェアの故障時のサポート期間(保守期間)が{5 年}以上であること。
関連する技術		
アクセシビリティ	JIS X8341 シリーズ ISO 9241-20 ISO/IEC 10779	

5.8.3.パーソナルコンピュータの機能要件・非機能要件

機能要件		
1	基本	共通オペレーション環境を利用できること。

5.8.3.1.デスクトップ型

非機能要件（個別の要件がある場合のみ記述）		
性能	基本	CPU の動作周波数は、{1. 0} GHz 以上であること。 チップ上のキャッシュメモリは{4}MB 以上であること。 {2}つ以上のスレッドを同時実行できること。
	基本	主記憶容量は、{1}GB 以上内蔵すること。
	基本	{80}GB 以上のディスク装置を内蔵すること。
拡張性	基本	1000BASE−T、100BASE−TX 及び 10BASE−T に対応した LAN ポートを{1}ポート以上内蔵すること。
	基本	USB 2.0 端子を{3}個以上内蔵すること。
	基本	キーボードは PS2 接続又は USB 接続できること。
	加点	パーソナルコンピュータ単体でモデム機能を有しないこと。単体でモデム機能を有しないこと。
サイズ	基本	本体・キーボード等が（本体サイズ：横{60}cm、縦{40}cm、奥行き{40}cm、本体重量{10}kg）のサイズ・重量に収まっていること。
画面解像度	基本	{14}インチ{35.56cm}以上、横{1024}ピクセル以上、縦{768}ピクセル以上の解像度をもつ表示部を有すること。 ［従来タイプ］ ・4:3　又は　5:4（横：縦） ［ワイドタイプ］ ・8:5　又は　16:9（横：縦）
セキュリティ	加点	盗難防止ロック・ワイヤーに対応していること。
	加点	BIOS パスワードロック機能をもつこと。
	加点	ハードディスクパスワードロック機能をもつこと。
グリーン調達 （グリーンIT）	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品（「環境物品等の調達の推進に関する基本方針」において「電子計算機」に対して規定されている基本方針に適合した製品）であること。
	基本	国際エネルギースタープログラム（Ver5.0）に適合し、主管省庁に届け出を行い、登録が行われた製品であること。
内蔵ドライブ	加点	DVD スーパーマルチ 2 層対応ドライブ（{8}倍速以上の DVD−R、{4}倍速以上の DVD−RW、{24}倍速以上の CD−R、{10}倍速以上の CD−RW）を内蔵する又は外付けできること。

マウス	加点	スクロール機能を有する 400 カウント以上の 2 つボタン式で光学方式の USB 接続ができること。
キーボード	基本	JIS 標準配列(109 キー)又は、OADG 準拠(109 キー)相当で、USB 又は PS2 接続にてパーソナルコンピュータ本体と接続可能なキーボードが添付されていること。

5.8.3.2.ノートブック型

非機能要件(個別の要件がある場合のみ記述)		
性能	基本	CPU の動作周波数は、{1.0}GHz 以上であること。 チップ上のキャッシュメモリは{4}MB 以上であること。 {2}つ以上のスレッドを同時実行できること。
	基本	主記憶容量は、{1}GB 以上内蔵すること。
	基本	{80}GB 以上のディスク装置を内蔵すること。
拡張性	基本	1000BASE-T、100BASE-TX 及び 10BASE-T に対応した LAN ポートを{1}ポート以上内蔵すること。
	基本	USB 2.0 端子を{2}個以上内蔵すること。
	加点	クライアント PC 単体でモデム機能を有しないこと。
サイズ	基本	本体・キーボード等が(本体サイズ:横{60}cm、縦{5}cm、奥行き{40}cm、本体重量{5}kg)のサイズ・重量に収まっていること。
画面解像度	基本	{14}インチ{35.56cm}以上、横{1024}ピクセル以上、縦{768}ピクセル以上の解像度をもつ表示部を有すること。
可用性	加点	防滴等に対して強度を確保していること。
セキュリティ	基本	盗難防止ロック・ワイヤーに対応していること。
	加点	BIOS パスワードロック機能をもつこと。
	加点	ハードディスクパスワードロック機能をもつこと。
電池容量	加点	電池容量 JEITA バッテリー動作測定法で{2}時間以上動作すること。
グリーン調達(グリーンIT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「電子計算機」に対して規定されている基本方針に適合した製品)であること。
	基本	国際エネルギースタープログラム(Ver5.0)に適合し、主管省庁に届け出を行い、登録が行われた製品であること。
内蔵ドライブ	加点	DVD スーパーマルチ 2 層対応ドライブ({8}倍速以上の DVD-R、{4}倍速以上の DVD-RW、{24}倍速以上の CD-R、{10}倍速以上の CD-RW)を内蔵する又は外付けできること。
マウス	加点	スクロール機能を有する{400}カウント以上の{2}つボタン式で光学方式の USB 接続ができること。
キーボード	基本	JIS 標準配列(87 キー)又は、OADG 準拠(86 キー)相当のキーボード

		をパーソナルコンピュータ本体に内蔵していること。

5.8.3.3.携帯用ノートブック型

非機能要件（個別の要件がある場合のみ記述）		
性能	基本	CPU の動作周波数は、{1.0}GHz 以上であること。 チップ上のキャッシュメモリは{4}MB 以上であること。 {2}つ以上のスレッドを同時実行できること。
	基本	主記憶容量は、{1}GB 以上内蔵すること。
	基本	{80}GB 以上のディスク装置を内蔵すること。
拡張性	基本	1000BASE-T、100BASE-TX 及び 10BASE-T に対応した LAN ポートを{1}ポート以上内蔵すること。
	基本	USB 2.0 端子を{2}個以上内蔵すること。
	加点	クライアント PC 単体でモデム機能を有しないこと。
サイズ	基本	本体・キーボード等が(本体サイズ：横{40}cm、縦{5}cm、奥行き{40}cm、本体重量{5}kg)のサイズ・重量に収まっていること。
画面解像度	基本	横{1024}ピクセル以上、縦{768}ピクセル以上の解像度をもつ表示部を有すること。
可用性	加点	防滴等に対して強度を確保していること。
	加点	盗難防止ロック・ワイヤーに対応していること。
セキュリティ	加点	BIOS パスワードロック機能をもつこと。
	加点	ハードディスクパスワードロック機能をもつこと。
電池容量	加点	電池容量 JEITA バッテリー動作測定法で{2}時間以上動作すること。
グリーン調達(グリーン IT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「電子計算機」に対して規定されている基本方針に適合した製品)であること。
	基本	国際エネルギースタープログラム(Ver5.0)に適合し、主管省庁に届け出を行い、登録が行われた製品であること。
ドライブ	加点	DVD スーパーマルチ 2 層対応ドライブ({8}倍速以上の DVD-R、{4}倍速以上の DVD-RW、{24}倍速以上の CD-R、{10}倍速以上の CD-RW)を内蔵する又は外付けできること。
マウス	加点	スクロール機能を有する{400}カウント以上の{2}つボタン式で光学方式の USB 接続ができること。
キーボード	基本	JIS 標準配列(85 キー)又は、OADG 準拠(85 キー)相当のキーボードをパーソナルコンピュータ本体に内蔵していること。

関連する技術	
ハードウェア	OADG テクニカルリファレンス(ハードウェア)
省電力	国際エネルギースタープログラム（Ver5.0)

周辺機器接続	USB 2.0
ディスプレイ接続	アナログ RGB (D-Sub 15 ピン), DVI-D, HDMI, DisplayPort
有線 LAN	1000BASE-T/100BASE-TX/10BASE-T
無線 LAN	IEEE 802.11a/b/g/n
Bluetooth	Bluetooth 2.1+EDR

5.8.4.シンクライアント・シンクライアントサーバの機能要件・非機能要件

5.8.4.1.シンクライアント

シンクライアントとは構成要素の一部をネットワーク上のシステムにもつ端末である。シンクライアントにはストレージ機能のみをネットワーク上にもつモデルや、画面表示と利用者からの入力を除くすべての処理をネットワーク上のサーバが担うモデル等がある。

機能要件		
1	基本	シンクライアントサーバに接続できること。
2	基本	サーバ上(一部クライアント側も含む場合もある)で共通オペレーション環境を利用できること。
3	基本	本体内に利用者が使用する情報の記録可能な媒体(ハードディスク等)を搭載していないこと。

5.8.4.2 シンクライアントサーバ

シンクライアントサーバとは、共通オペレーション環境を提供し、ネットワークを経由しシンクライアントからの接続を受け付けるサーバである。単一 OS インスタンスで複数セッションを受け付ける方式、セッションごとに仮想マシンを用意する方式、個々の接続に対して個別ハードウェアを割り当てるブレード方式等がある。

機能要件		
1	基本	パーソナルコンピュータとシンクライアントからのアクセスができること。

5.8.5.共通オペレーション環境の定義

共通オペレーション環境とは、ハードウェアの管理、アプリケーションの実行、ファイル操作等を行うソフトウェア・システムを指す。パーソナルコンピュータやシンクライアントサーバはこの環境を利用できる。共通オペレーション環境の機能・サービスを以下に示す。

共通オペレーション環境	
機能・サービス	定義
OS	オペレーティングシステムとして基本的な CPU・メモリ等の資

	源管理・アクセス管理等を行う。
ウイルス対策	記憶装置上にウイルスがないか定期的に確認し、また、ファイル入出力やネットワーク通信を常時監視し、コンピュータウイルスによる侵入等を検知した場合に、駆除等の必要な作業を行う。
Web ブラウザ	Web ブラウザとは WWW を閲覧する。
パーソナルファイアウォール・検疫	インバウンド及びアウトバウンドの通信を監視し、許可されたアプリケーションからの通信のみを疎通させる。
画像処理	画像の作成、加工を行う。
文書作成	文書の作成、加工を行う。
プレゼンテーション	スライドの作成、加工を行う。
表計算	表の作成、計算、加工を行う。
メールクライアント	メールの送受信を行う。
動画閲覧	動画ファイルを閲覧する。
Web 作成	HTML の編集と Web サイトへの発行を行う。
電子的な印刷文書の作成	仮想プリンタを通じて印刷機能をもつアプリケーションから電子的な印刷文書を作成する。
コマンドライン環境	コマンドライン及びバッチでファイル操作、設定変更等の作業を行う。
日本語文字入力(かな漢字変換)	日本語の入力をローマ字入力及びかな入力の方式で行い、漢字に変換できる。
ソフトウェア配布受信	ソフトウェア管理サーバからソフトウェア及び修正プログラムの受け取る機能を有する。
インベントリ情報取得	端末に導入されているソフトウェア、修正プログラム、アンチウイルスソフトウェアのシグニチャ、利用者が保管しているファイル等について目録を作成し、サーバに送信する。
暗号化	システム、ファイル、パスワード等に暗号化を行う。
情報漏えい対策	USB メモリ等を通じた情報複製を抑止する。

関連する技術	
Web ブラウザ	HTTP, FTP, SSL/TLS, Java Script HTML 4.1
文書作成 プレゼンテーション 表計算	ISO/IEC 26300 Open Document Format (ODF) ISO/IEC 29500 Office Open XML Format (OOXML)
静止画	JPEG, GIF, PNG
動画	MPEG-1, MPEG-2, MPEG-4/H.264, SMPTE VC-1
印刷文書	Adobe Portable Document Format Version 1.7 (PDF) ECMA-388 XML Paper Specification (XPS)
圧縮文書	ZIP

5.8.5.1. OS の機能要件・非機能要件

OS は、オペレーティングシステムとして基本的な CPU・メモリ等の資源管理・アクセス管理等を行う機能を有する。

機能要件		
1	基本	CPU 利用率の稼動データが収集できること。
2	基本	物理ハードディスクの使用率を収集できること。
3	基本	物理ハードディスクの入出性能情報が収集できること。
4	基本	物理メモリの空き容量の情報が収集できること。
5	基本	仮想メモリの空き容量の情報が収集できること。
6	基本	プロセスの同時起動数が収集できること。
7	基本	プロセスごとの CPU 利用率、仮想メモリ使用率が収集できること。
8	基本	ネットワークインタフェースカードの入出力情報が収集できること。
9	基本	システムのイベントを記録し監視ができること。
10	基本	OS で実行されているサービス(デーモンプロセス)の状態を監視できること。
11	基本	収集データは内部統制監査に必要な期間分のデータの保存ができること。
12	基本	マルチユーザモード(一般ユーザ、管理者ユーザ等)での利用ができること。
13	基本	機器情報【CPU、メモリ、物理ディスク、論理ディスク、MAC アドレス、外部装置等】が閲覧できること。
14	基本	導入されているソフトウェアの情報を閲覧できること。
15	基本	OS に関する情報【OS、バージョン、コンピュータ名、IP アドレス等のネットワーク情報等】が閲覧できること。

非機能要件		
バックアップ	基本	収集したデータは必要に応じて外部記憶装置に退避させ、必要なときに復旧できること。

5.8.5.2.ウイルス対策の機能要件・非機能要件

ウイルス対策では、記憶装置上にウイルスがないか定期的に確認し、また、ファイル入出力やネットワーク通信を常時監視し、コンピュータウイルスによる侵入等を検知した場合に、駆除等の必要な作業を行う。要件は 5.9.7.1 を参照のこと。

5.8.5.3.Web ブラウザの機能要件・非機能要件

Web ブラウザは、WWW を閲覧する機能を有する。なおコンテンツフィルタリング機能については 5.9.7.2 を参照のこと。

機能要件		
1	基本	Web サーバと通信して指定された URI から情報を取り出すことができること。
2	基本	W3CHTML 標準、ECMA スクリプト規格に規定された機能のみを用いて作成された

		ウェブコンテンツの表示及びフォームを通じての入力ができること。
3	基本	JPEG、GIF 及び Adobe Flash 形式の画像データを表示できること。
4	基本	画像の自動ダウンロードの制御ができること。
5	基本	ポップアップの制御ができること。
6	基本	フィッシングサイト URL へのアクセス制御ができること。
7	基本	エンコードの選択ができること。

5.8.5.4.ファイアウォール・検疫の機能要件・非機能要件

ファイアウォールは、インバウンド及びアウトバウンドの通信を監視し、許可されたアプリケーションからの通信のみを疎通させる機能を有する。

機能要件		
1	基本	ポート番号等に基づき通信の許可及び拒否を制御できること。
2	基本	IPv4 及び IPv6 の両方のプロトコルに対応していること。
3	基本	ログを記録ができること。

非機能要件		
パフォーマンス	基本	多量のパケットを受信したときの通常の処理が続けられること。
可用性	基本	ログの増加により機能停止しないこと。

5.8.5.5.画像処理の機能要件

画像処理は、画像の作成、加工を行う機能を有する。ここでいう画像とは、標準技術のところで挙げた諸標準に準拠したフォーマットの画像を指すこととする。

機能要件		
1	基本	画像ファイルの読み込みができること。
2	基本	画像の作成ができること。
3	基本	画像の加工【切り取り、コピー、貼(は)り付け、色の編集、サイズの変更　等】ができること。

5.8.5.6.文書作成の機能要件

文書作成は、文書の作成、加工を行う機能を有する。

機能要件		
1	基本	文書の作成を行えること。
2	基本	文書の加工【切り取り、コピー、貼(は)り付け、色の編集　等】を行えること。
3	基本	複数回の改行入力を行うことなく自由な位置から文書を書き出せること。
4	基本	縦書き表記に対応できること。
5	加点	画像ファイルの読み込みができること。
6	加点	標準フォーマットで保存できること。

5.8.5.7.プレゼンテーションの機能要件

プレゼンテーションは、スライドの作成、加工を行う機能を有する。

機能要件		
1	基本	スライドの作成を行うことができること。
2	基本	スライドの加工【切り取り、コピー、貼(は)り付け、色の編集　等】を行えること。
3	基本	スライドショーを実行できること。
4	加点	画像ファイルの読み込みができること。
5	加点	音声ファイルの読み込みができること。
6	加点	動画ファイルの読み込みができること。
7	加点	標準フォーマットで保存できること。

5.8. 5.8.表計算の機能要件

表計算は、表の作成、計算、加工を行う機能を有する。

機能要件		
1	基本	表の作成を行えること。
2	基本	表の計算(演算子や基本関数の利用を含む)を行えること。
3	基本	表の加工【切り取り、コピー、貼(は)り付け、色の編集、行列の追加・削除　等】を行えること。
4	基本	表上のデータ値からグラフを作成できること。
5	基本	グラフの加工【軸の設定等、色の編集　等】ができること。
6	加点	画像ファイルの読み込みができること。
7	加点	標準フォーマットで保存できること。

5.8.5.9.メールクライアントの機能要件

メールクライアントは、メールの送受信を行う機能を有する。

機能要件		
1	基本	一般的なメールサーバで使われるプロトコル(SMTP、POP3、IMAP)で接続できること。
2	基本	送信者、宛先(あてさき)、件名、本文、日付の組み合わせで全文検索が行えること。
3	基本	転送設定が行えること。
4	基本	不在通知設定が行えること。
5	基本	Webビーコン対策として電子メール本文中に表示される画像の自動ダウンロードが制御できること。
6	基本	ローカル保存データを暗号化できること。
7	基本	ウイルス感染の可能性のあるファイルの添付を拡張子単位でブロックできること。
8	基本	メール本文及び添付された文書の暗号化に対応しており、利用可能な機能(印刷等)の制限ができること。

9	基本	SMTP 認証に対応できること。
10	基本	アドレス帳が LDAP と連携して表示できること。
11	基本	アドレス帳の一部を入力すると補完するオートコンプリート機能に対応すること。
12	基本	暗号化されたメールボックス、アドレス帳であっても使用できること。
13	基本	開封確認付きメールに対応できること。
14	基本	HTML メールは、テキスト形式又はリッチテキスト形式として閲覧できる機能を有すること。
15	基本	HTML メールを表示する場合にブラウザを使わずに表示できること。
16	基本	SPAM メールをフィルタリングする機能を有すること。
17	基本	添付ファイルの有無を容易に判別ができること。
18	基本	メール本文や件名等の文中に特定文字列、送信者情報等により自動的にフォルダ分類できること。
19	基本	メールを件名順、日付順、送信元ユーザ順等でソートできること。
20	基本	メールデータをテキスト形式又は汎用的なフォーマットでエクスポートが可能なこと。
21	基本	アドレス帳を CSV 形式又は vCARD 形式等の汎用的なフォーマットでエクスポート及びインポートができること。
22	基本	メールボックスの最適化ができること。

5.8.5.10.動画閲覧の機能要件

動画閲覧は、動画ファイルを閲覧する機能を有する。

機能要件		
1	基本	MPEG1、MPEG2 及び MPEG4 規格に準拠したフォーマットの動画、音声、静止画の表示を行えること。

5.8.5.11.Web 作成の機能要件

Web 作成は、HTML の編集と Web サイトへの発行を行う機能を有する。

機能要件		
1	基本	HTML の編集ができること。
2	基本	Web サイトへの発行ができること。

5.8.5.12.コマンドライン環境の機能要件

コマンドライン環境は、コマンドライン及びバッチでファイル操作、設定変更等の作業を行う機能を有する。

機能要件		
1	基本	コマンドラインでファイル操作、設定変更等の作業を行うことができること。
2	基本	バッチ処理ができること。

5.8.5.13.日本語文字入力(かな漢字変換)の機能要件

日本語入力は、日本語の入力をローマ字入力及びかな入力の方式で行い、漢字に変換できる機能を有する。

機能要件		
1	基本	連文節変換、学習機能、単語登録、ローマ字／かな入力等一般的に日本語入力に必要とされる基本的な機能を有していること。
2	基本	漢字に変換できる機能を有すること。
3	基本	少なくとも、JIS X 0208 の文字セットが入力できること。
4	加点	同音異義語等についてはその意味の違いや文例を表示できること。
5	加点	郵便番号から住所への変換、日付入力に対する支援機能を有していること。

5.8.5.14.ソフトウェア配布受信の機能要件

ソフトウェア管理サーバからソフトウェア及び修正プログラムの受け取る機能を有する。

機能要件		
1	基本	ソフトウェア管理サーバからソフトウェア及び修正プログラム(ウイルスのパターンファイルも含む)の受信ができること。
2	基本	受信したソフトウェア及び修正プログラムの結果を確認できること。
3	基本	受信・実行後に再起動が必要な場合は、作業している利用者に再起動を促すメッセージを表示できること。
4	加点	受信したソフトウェア及び修正プログラムを実行時に、利用者の作業を中断しないようにGUI 表示しない、又は GUI を隠すことができるようにすること。
5	加点	主要インストーラの形式でのセットアップに対応可能なこと。

5.8.5.15.インベントリ情報取得の機能要件

インベントリ情報取得は、端末に導入されているソフトウェア、修正プログラム、アンチウイルスソフトウェアのシグニチャ、利用者が保管しているファイル等について目録を作成し、サーバに送信する機能を有する。

機能要件		
1	基本	端末に導入されているソフトウェア、修正プログラム、アンチウイルスソフトウェアのシグニチャ、利用者が保管しているファイル等について目録を作成し、サーバに送信できること。

5.8.5.16.暗号化の機能要件・非機能要件

暗号化は、ファイル、パスワード等の暗号化を行う機能を有する。

機能要件		
1	基本	ハードディスクを自動的に暗号化し、認証基盤と連携して復号鍵を使って集約管理できること。
2	基本	認証基盤と連携し、ファイル単位で暗号化を行えること。
3	基本	認証基盤と連携し、フォルダ単位で暗号化を行えること。
4	基本	簡易な操作で暗号化・復号化できること。
5	基本	外部媒体にファイルを格納する際に容易にファイルを暗号化できること。

非機能要件		
バックアップ	基本	暗号化を行った端末が何らかの理由で破損した場合でも、バックアップしておいた復号鍵等を使用して暗号化したファイルを復号できること。

5.8.5.17.情報漏えい対策の機能要件

情報漏えい対策は、情報漏えいを防止する機能を有する。

機能要件		
1	基本	認証基盤と連携し、機密文書のアクセス(閲覧・印刷・更新等)をファイル単位で制御できること。
2	加点	認証基盤と連携し、USB メモリ等の外部媒体を通じた情報複製を抑止できること。
3	加点	認証基盤と連携し、電子メールの添付ファイルの送信・転送等を抑止できること。

5.8.6.オフィスプリンタ装置の機能要件・非機能要件

オフィスプリンタ装置とは、事務所に置く印刷デバイスである。データ処理装置として、文字・図形・写真等を用紙上に記録する機能のみをもつ共有型装置をプリンタとし、個別の PC に接続し占有する装置を小型プリンタとし、プリンタとしての機能に加えコピー機、スキャナ、ファクシミリ等の機能を併せ持つ装置を複合機と定義する。

5.8.6.1.プリンタの機能要件、非機能要件

プリンタとはデータ処理装置として、文字・図形・写真等を用紙上に記録する共有型の印刷装置である。

機能要件		
1	基本	端末からの指示に基づいてデータを紙に印字することができること。
2	基本	複数ページの文書を印刷する際、ページ順の並べ替え並びに綴(と)じることができること。
3	加点	部数印刷をする際に、電子的な手段で並べ替え、帳合い等が可能なこと。
4	基本	文書の印刷をする際、入力原稿の形式に係らず、複数ページをまとめて(N-Up、両面、モノクロ)で印刷ができること。
5	選択	シンクライアント環境下において、機能制限(用紙指定、部数、両面、帳合い、ページ揃(そろ)え等)のないこと。
6	加点	プリントデータのネットワーク帯域削減手段があること。

非機能要件（個別の要件がある場合のみ記述）		
印刷速度	基本	毎分 A4 ｛白黒：30、カラー30｝ページ以上で印刷できること。
用紙サイズ	基本	(A3、A4)サイズまで印刷できること。
カラー	選択	多色刷り・カラー印刷ができること。
解像度	基本	｛1200｝dpi 相当以上で印刷できること。
印字方式	基本	レーザー又は LED 又はインクジェット又は昇華型熱転写であること。
最大消費電力	基本	｛2.0k｝W 以下であること。
サイズ	基本	本体サイズは幅｛1200｝mm×奥行き｛1000｝mm×高さ｛1500｝mm 以下であること。
重量	基本	本体重量は｛300｝kg 以下であること。
電源	基本	特別な電源工事を必要としないこと(日本にあっては、AC 100V 50/60Hz 共用、最大消費電力 1.5kW/1 口以下)。
トレイ容量	基本	オートシートフィーダを使用でき、給紙可能枚数は｛500｝枚以上であること。
インタフェース	基本	標準パラレル (EPP/ECP), USB 接続のいずれか、又は両方のインタフェースをもつこと。
	基本	ネットワーク上の情報システムに接続するためのインタフェース(10BASE-T, 100BASE-TX, 1000 BASE-T 等)をもつこと。
セキュリティ	加点	印刷物の取り出しに制限機能をもつこと。
	加点	データの受信(印刷)に IP アドレスで制限がかけられること。
	加点	設定情報等へのアクセスに認証機能をもつこと。

	加点	機器へ保存された印刷データを再生不可能な形で削除する機能をもつこと。
管理	加点	遠隔操作により状態確認、設定の可能な機能をもつこと。
	加点	複数台の機器の状態・設定及び印刷枚数の統合的管理機能をもつ手法を提供可能なこと。
	加点	ユーザ・グループにより使用可能な機能【カラー印刷】に制限機能をもつこと。
	加点	単一のインストールプログラムからドライバがインストールできること。
グリーン調達(グリーンIT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「プリンタ」に対して規定されている基本方針に適合した製品)であること。
	基本	国際エネルギースタープログラムに適合し、主管省庁に届け出を行い、登録が行われた製品であること。
	加点	エコマークを取得した製品であること。

5.8.6.2.小型プリンタの機能要件、非機能要件

小型プリンタとはデータ処理装置として、文字・図形・写真等を用紙上に記録する占有型の印刷装置である。

機能要件		
1	基本	端末からの指示に基づいてデータを紙に印字することができること。
2	基本	文書の印刷をする際入力原稿の形式に係らず、複数ページをまとめて(N−Up、モノクロ)で印刷できること。
3	加点	文書の印刷をする際入力原稿の形式に係らず、複数ページをまとめて両面で印刷できること。
4	選択	シンクライアント環境下において、機能制限(用紙指定、部数等)のないこと。
5	加点	プリントデータのネットワーク帯域削減手段があること。

非機能要件（個別の要件がある場合のみ記述）		
印刷速度	基本	毎分 A4 ｛白黒：10、カラー10｝ページ以上で印刷できること。
用紙サイズ	基本	(A3、A4)サイズまで印刷できること。
カラー	選択	多色刷り・カラー印刷ができること。
解像度	基本	｛1200｝dpi 相当以上で印刷できること。
印字方式	基本	レーザー又は LED 又はインクジェット又は昇華型熱転写であること。
最大消費電力	基本	モバイル型にあっては｛30｝W、据え置き型にあっては｛450｝W 以下であること。
サイズ	基本	本体サイズはモバイル型にあっては幅｛350｝mm×奥行き｛180｝mm×高さ｛85｝mm、据え置き型にあっては、幅｛450｝mm×奥行き｛450｝mm×高さ｛450｝mm 以下であること。
重量	基本	本体重量はモバイル型にあっては(2.2)kg、据え置き型にあっては｛20｝kg 以下であること。

電源	基本	特別な電源工事を必要としないこと(日本にあっては、AC 100V 50/60Hz 共用、最大消費電力 1.5kW/1 口以下)。
	加点	AC(100-240)V に対応可能であること。海外での使用も考慮し、電源プラグアダプタを提供すること。
トレイ容量	基本	オートシートフィーダを使用でき、給紙可能枚数は{30}枚以上であること。
インタフェース	基本	標準パラレル (EPP/ECP), USB 接続のいずれか、又は両方のインタフェースをもつこと。
	加点	ネットワーク上の情報システムに接続するためのインタフェース(10BASE-T, 100 BASE-TX 等)をもつこと。
セキュリティ	加点	データの受信(印刷)に IP アドレスで制限がかけられること。
	加点	機器へ保存された印刷データを再生不可能な形で削除する機能をもつこと。
管理	加点	機器の状態・設定及び印刷枚数の管理機能をもつ手法を提供可能なこと。
	加点	単一のインストールプログラムからドライバがインストールできること。
グリーン調達(グリーン IT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「プリンタ」に対して規定されている基本方針に適合した製品)であること。
	基本	国際エネルギースタープログラムに適合し、主管省庁に届け出を行い、登録が行われた製品であること。
	加点	エコマークを取得した製品であること。

5.8.6.3.複合機の機能要件、非機能要件

複合機とは、プリンタ機能に加えコピー、スキャナ、ファクシミリ、及び、電子原稿蓄積機能を併せ持つ装置である。

機能要件		
1	基本	端末からの指示に基づいてデータを紙に印字することができること。
2	基本	紙の文書を複写できること。
3	基本	複数ページの文書を印刷する際、ページ順の並べ替え並びに綴(と)じることができること。
4	基本	スキャナで文書を読み取り、電子化できること。
5	基本	ファクシミリ搭載機は電話回線に接続し、ファクシミリを送受信できること。
6	基本	スキャナ、ファクシミリの電子文書を本体内に一時保存し、操作によって参照、取り出し、削除が可能なこと。
7	基本	文書の印刷/複写をする際入力原稿の形式に係らず、複数ページをまとめて(N-Up、両面、モノクロ)で印刷/複写ができること。
8	選択	シンクライアント環境下において、機能制限(用紙指定、部数、両面、帳合い、ページ揃(そろ)え等)のないこと。
9	加点	プリントデータのネットワーク帯域削減手段があること。

非機能要件(個別の要件がある場合のみ記述)

印刷速度	基本	毎分 A4 ｛白黒：30、カラー30｝ページ以上で印刷できること。
用紙サイズ	基本	(A3、A4)サイズまで印刷できること。
カラー	選択	多色刷り・カラー印刷ができること。
解像度	基本	｛1200｝dpi 相当以上で印刷できること。
印字方式	基本	レーザー又は LED 又はインクジェット又は昇華型熱転写であること。
最大消費電力	基本	｛2.0k｝W 以下であること。
サイズ	基本	本体サイズは幅｛1200｝mm×奥行き｛1000｝mm×高さ｛1500｝mm 以下であること。
重量	基本	本体重量は｛300｝kg 以下であること。
電源	基本	特別な電源工事を必要としないこと(日本にあっては、AC 100V 50/60Hz 共用、最大消費電力 1.5kW/1 口以下)
トレイ容量	基本	オートシートフィーダを使用でき、給紙可能枚数は｛500｝枚以上であること。
コピー機能	選択	カラー、モノクロコピーの選択が可能であること。
自動原稿送り装置	基本	スキャン、ファクシミリ送信、複写時に自動的に複数の(片面、両面、異種サイズ)原稿を読み取ることができること。
ファクシミリ機能	基本	ファクシミリ番号の登録・管理が可能であること。
スキャン機能	基本	データを電子メールに添付可能であること。
	基本	データを本体又はネットワーク上の個人フォルダ又は共有フォルダへ格納可能できること。
	基本	機器内に一時保存されたデータをネットワークを介して端末から参照、読み取り、削除等の操作が可能なこと。
	基本	カラー、モノクロスキャンの選択が可能であること。
	基本	指定した解像度【200dpi,400dpi,600dpi 等】でスキャンが可能であること。
	基本	スキャンデータの保存形式(PDF, XPS, JPEG,TIFF 等)が選択可能であること。
インタフェース	基本	標準パラレル (EPP/ECP), USB 接続のいずれか、又は両方のインタフェースをもつこと。
	基本	ネットワーク上の情報システムに接続するためのインタフェース(10BASE-T, 100BASE-TX 等)をもつこと。
セキュリティ	加点	印刷物の取り出しに制限機能をもつこと。
	加点	データの送受信(スキャン、印刷)に IP アドレスで制限がかけられること。
	加点	設定情報等へのアクセスに認証機能をもつこと。
	加点	機器へ保存された【コピー、ファクシミリ、スキャン、印刷データ 等】の印刷データを再生不可能な形で削除する機能をもつこと。
管理	加点	遠隔操作により状態確認、設定の可能な機能をもつこと。
	加点	複数台の機器の状態・設定及び印刷枚数の統合的管理機能をもつ手法を提供可能なこと。
	加点	ユーザ・グループにより使用可能な機能(カラー印刷、スキャン機能、ファクシミリ機能等)に制限機能をもつこと。
	加点	単一のインストールプログラムからドライバがインストールできること。
グリーン調達(グリーン IT)	基本	「国等による環境物品等の調達の推進等に関する法律」に基づく基本方針に適合した製品(「環境物品等の調達の推進に関する基本方針」において「コピー機」に対して規定されている基本方針に適合した製品)であること。

	基本	国際エネルギースタープログラムに適合し、主管省庁に届け出を行い、登録が行われた製品であること。
	加点	エコマークを取得した製品であること。

5.8. 7.仮想化への対応

機能要件（仮想化環境への対応）		
1	基本	仮想化機構により実現された仮想化ゲストサーバ、仮想化ストレージ、仮想化ネットワークなどから構成される仮想化環境において物理サーバ環境と同等のソフトウェアを配置でき、同等の機能を満たすことができること。

5.9.運用管理 / セキュリティ

運用管理とは、主にコンピュータ上で稼動し、様々なサービスを提供しているシステムが、想定外の要因によって停止することなく利用顧客に対してサービスを提供できるよう当該環境を維持管理することである。

また、セキュリティとは、ウイルスや不正アクセス等の内外要因から情報資産を守り、誰もが安心してコンピュータを利用できる環境を構築、維持することである。

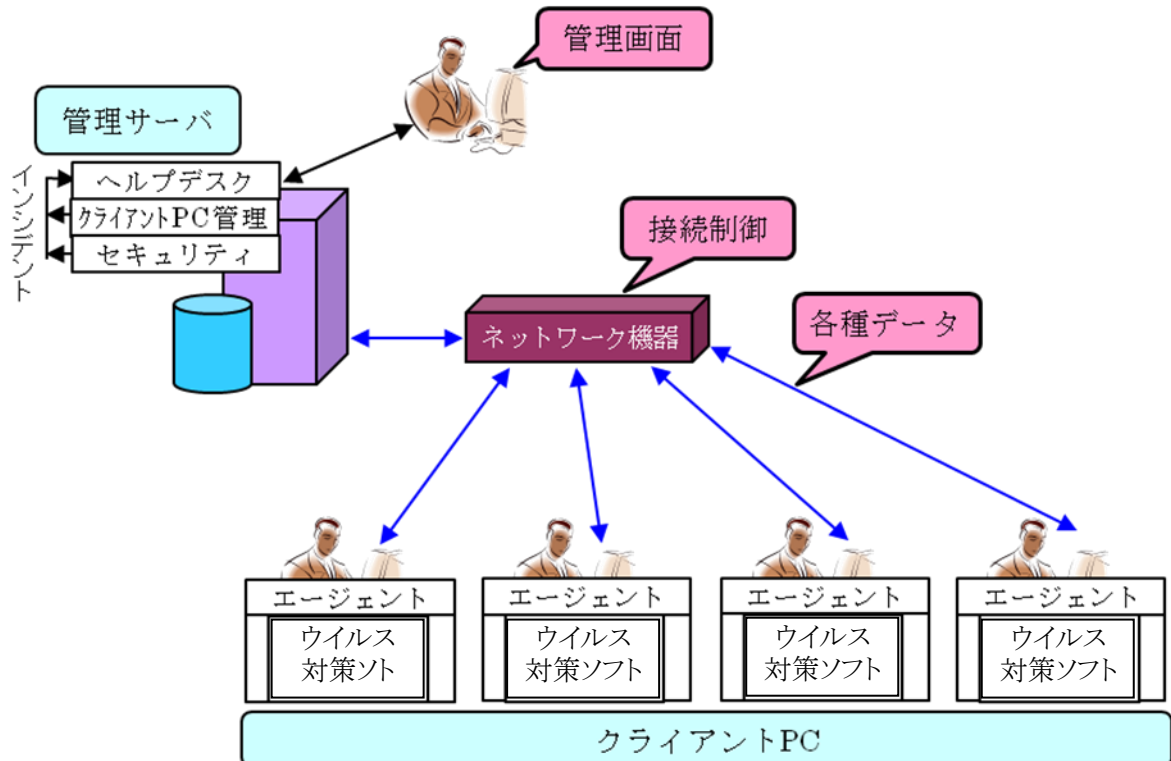



図 5.9-1 運用管理概要図(クライアント PC 系)

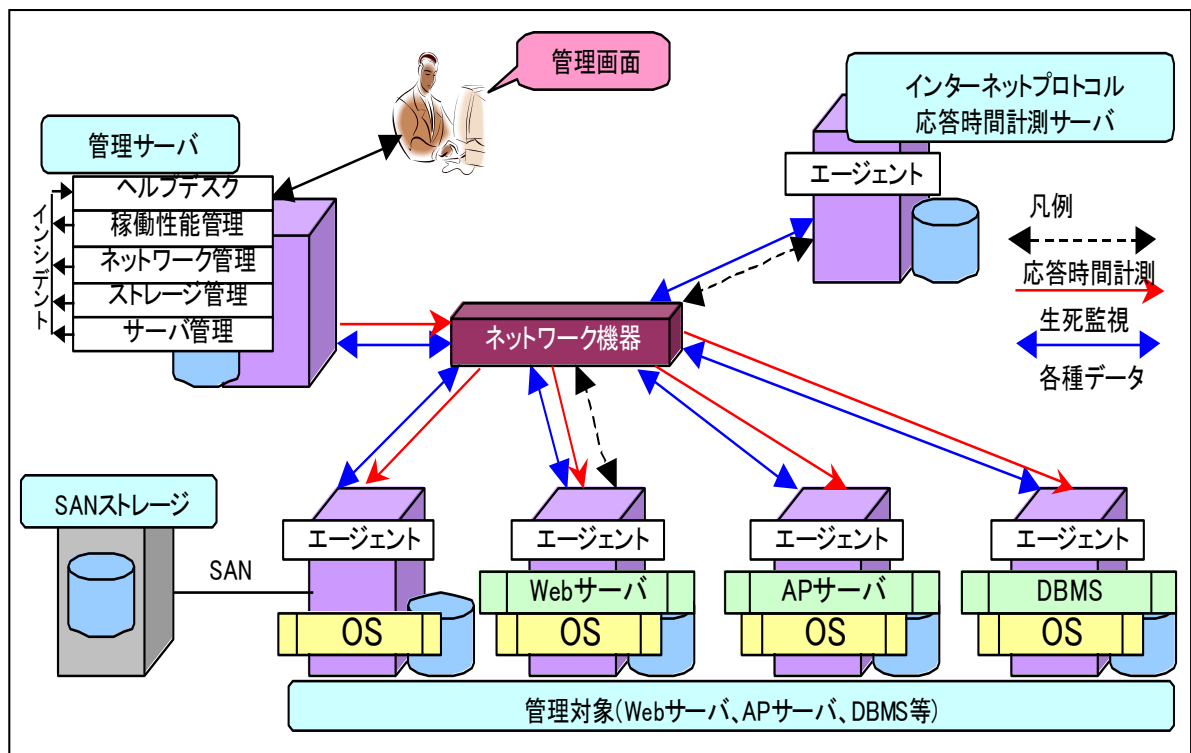



図 5.9-2 運用管理概要図(サーバ系)

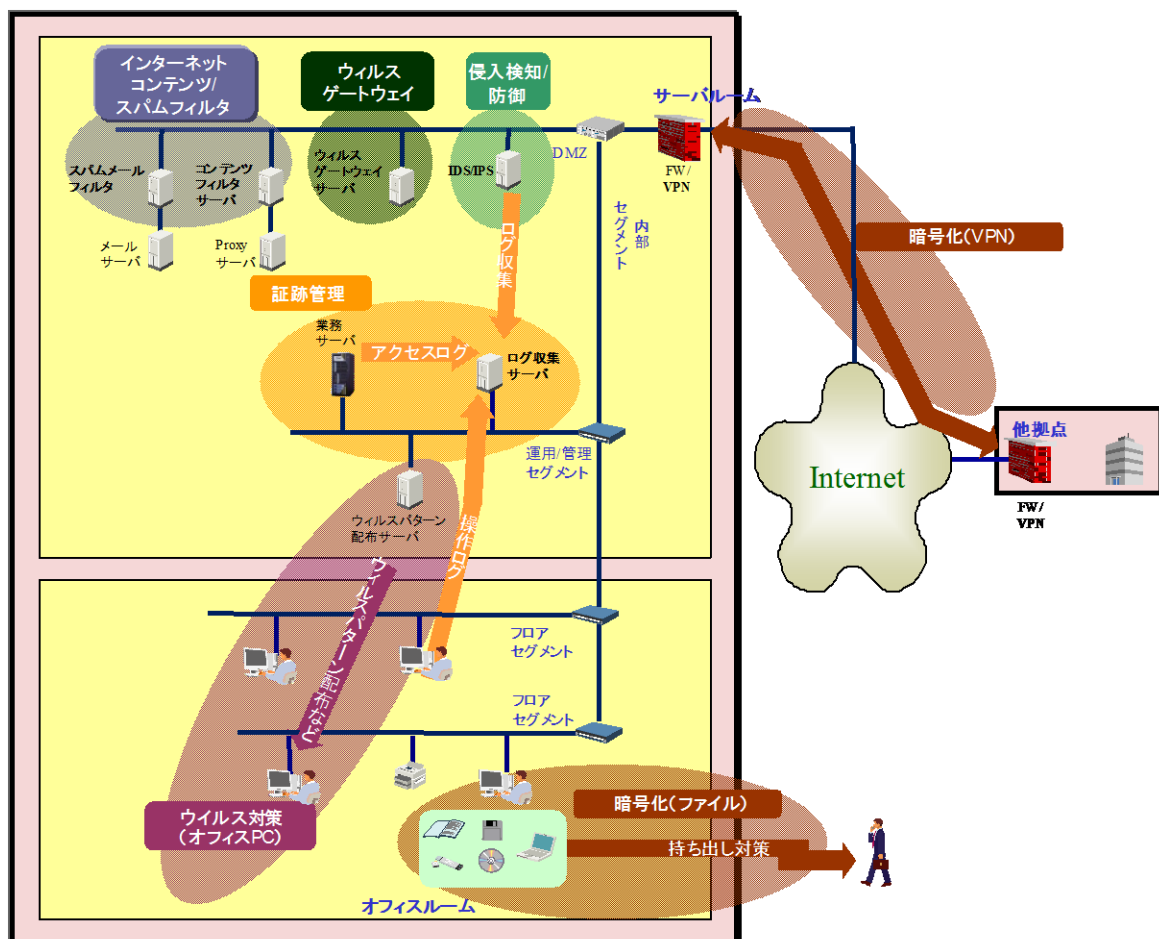



図 5.9-3 セキュリティ概要図

運用管理/セキュリティの機能・サービスと定義は次の通りである。

機能・サービス	定義
稼動性能管理	稼動性能管理では、OS やアプリケーションの稼動性能情報を一元的に管理する機能を有する。また、収集した稼動データを用いて、障害時の原因究明の支援を行う。
クライアント PC 管理	クライアントPC 管理では、ネットワークで接続可能な環境に配置されたクライアントPC のハードウェア構成情報、導入ソフトウェア情報、OS 情報の一元的な収集並びに管理を実現する構成管理機能、ネットワーク接続された PC に対するソフトウェアの導入・削除を実現する資源配布機能、同 PC をリモート操作する遠隔操作機能を有する。
サーバ管理	サーバ管理では、府省内に設置された情報システムの業務サーバ及び部門内に個別に設置された File サーバ等の稼動状況や負荷状況を監視、災害等によるデータ破壊に備えた対応(遠隔地に複製システムを設置、バックアップメディアの遠隔地での保存等)、サーバ設置環境における付帯設備(無停電装置、ラック温度等)までを管理対象とし、システム運用管理者(又は、それに準ずる作業者)が携わる範囲を想定している。 ただし、府省内でサーバを運用せず外部に委託するアウトソーシングサービスを利用している場合や、データセンター事業者に関する要件(規模等)は考慮していない。
ネットワーク管理	ネットワーク管理では、下記内容を想定している。 (1)府省内のネットワークを構成する、L2−L3 機器(スイッチ、ルータ等)を中心としたネットワークの運用 (2)ICT システムの管理という観点で通常の府省情報システムの運用者が携わる範囲 (3)ネットワーク上で発生する障害の発生に対する迅速な復旧活動を支援するために必要な機能、障害によるビジネスの阻害を極小化するための機能、障害の未然防止に役立つ機能 ただし、NI/SI 事業者が保守代行をする場合の要件、iDC 事業者の要件等については考慮をしていない。
ストレージ管理	ストレージ管理では、データやプログラムを記憶する外部記憶装置(ストレージ装置)のリソースを効率的に一元管理し、構成表示、性能／状態監視、各種イベント通知を行う機能を有する。
サービスデスク	サービスデスクでは、情報システムのトラブルや使用方法等の問い合わせを一括して受け付ける機能を有する。電話やメール等で事象の受け付けをし、受け付けた内容をデータベースにして利用者も参照可能にすることができる。 また、他システムの障害管理機能や構成管理機能等と連携して、トラブル発生時の問題解決に利用することができる。
セキュリティ	セキュリティでは、コンピュータへの不正アクセス、ウイルス検知、コンテンツフィルタリングサーバ拒否状況等の情報セキュリティ上の問題となる事象について監視を行う。また、監視により検出された危険については、その危険度に応じた通報を行う機能を提供する。また、監視内容についてグラフ化された統計情報による報告及び分析、改善提案等を行う。
ジョブ管理	ジョブ管理では、定型的に行われる業務を手順化し、決められた間隔又は特定の事象を契機にジョブの実行をする。

5.9.1.稼動性能管理の機能/非機能要件

5.9.1.1.サーバ稼動情報の一元管理

サーバ稼動情報の一元管理は、監視対象を一元的に管理する機能である。

機能要件		
1	基本	OS、アプリケーションをまとめて一つの画面で管理できること。
2	基本	OS、アプリケーションの監視に関する操作は、すべて共通化していること。
3	基本	監視対象は階層化し、障害の発生箇所の特定をしやすくすること。
4	基本	監視項目の確認画面から、関連するレポート画面がすぐに呼び出せること。
5	基本	ユーザ権限により、操作する機能を限定できること。
6	基本	監視対象サーバの生死状態が監視できること。
7	加点	設定変更をした場合等の操作ログが取得できること。
8	基本	管理サーバと監視対象のプロセス稼動状況を監視できること。
9	加点	仮想化されたリソースの管理であっても簡便に一元管理が行えること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	管理サーバはクラスタ構成がとれること。
セキュリティ	基本	ログイン管理を行い、不当に設定情報等の変更がされないようにすること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。
バックアップ	基本	構成定義・操作ログのバックアップをすること。

5.9.1.2.稼動性能情報収集管理

稼動性能情報収集管理は、監視対象の稼動性能情報を収集し、異常を検知する機能である。

情報を収集し、異常を検知する場所は管理サーバ又は非監視側とする。

機能要件		
1	基本	デフォルトの監視項目(しきい値を含む)を有していること。
2	基本	監視項目は自由に作成できること。
3	基本	測定がしきい値を越えた場合、電子メールの発行やコマンドの実行が行えること。
4	加点	しきい値監視のみを行い、データを蓄積しない設定が行えること。
5	基本	収集したデータは定期的【時・日・週・月ごと】に集約することが可能なこと。
6	基本	指定した期間を越えた収集データは自動的に削除されること。
7	基本	ユーザ定義により、任意の測定データも取り込めること。
8	基本	管理サーバと監視エージェントの間で通信ができない状態でも、測定データの損失が発生しないこと。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	基本	監視定義のバックアップが行えること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.3.レポート管理

レポート管理は、収集した稼動性能データをグラフ化する機能である。

機能要件		
1	基本	グラフ化する場合、【棒グラフ、折れ線グラフ、円グラフ 等】、複数の表示形式を選択できること。
2	基本	レポートのひな形がデフォルトで用意されていること。

3	基本	レポートのひな形を自由に作成できること。
4	基本	OS、アプリケーションの各監視項目の測定データを一緒にグラフ化できること。
5	基本	過去のある時点のデータと、今のデータを重ねて同時に表示できること。
6	加点	レポートを表示した画面から、レポートをファイル保存できること。
7	基本	自動でレポートの保存や、測定データの保存ができること。
8	基本	表示したグラフの表示期間を自由に変更できること。

5.9.1.4.OS 稼動管理

OS 稼動管理は、OS に関する稼動性能情報を収集する機能である。

機能要件		
1	基本	CPU 利用率の稼動データが収集できること。
2	基本	マルチ CPU の場合、CPU ごとの稼動データが収集できること。
3	基本	マルチコア CPU の場合、コアごとに CPU の稼動データが収集できること。
4	基本	物理ハードディスクの使用率を収集できること。
5	基本	物理ハードディスクの入出力性能情報が収集できること。
6	基本	物理メモリの空き容量の情報が収集できること。
7	基本	仮想メモリの空き容量の情報が収集できること。
8	基本	プロセスの同時起動数が収集できること。
9	基本	プロセスごとの CPU 利用率、仮想メモリ使用率が収集できること。
10	基本	ネットワークインタフェースカードの入出力情報の収集ができること。
11	基本	イベントログの監視ができること。
12	基本	OS で実行されているサービス(デーモンプロセス)の状態を監視できること。

非機能要件（個別の要件がある場合のみ記述）		
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.5.DBMS 稼動管理

DBMS 稼動管理は、DBMS に関する稼動性能情報を収集する機能である。

機能要件		
1	基本	テーブルごとの使用状況が収集できること。
2	基本	発行されている SQL 文が収集できること。
3	基本	コネクションの状態が監視できること。
4	基本	SQL 文の発行元 IP アドレス・プログラムの情報が収集できること。
5	基本	ロックの発生状態を監視できること。
6	基本	入出力情報【回数　等】を収集できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	DB サーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.6.AP サーバ稼動管理

AP サーバ稼動管理は、AP サーバに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	アクセス数が収集できること。
2	基本	ガベージコレクションの回数が収集できること。
3	基本	ガベージコレクションの実行時間が収集できること。
4	基本	Java コンポーネント・.NET コンポーネント等のコンポーネントアプリケーションを実行するための基盤に含まれる仮想マシンのヒープ使用量が収集できること。
5	基本	Web サービスの平均応答時間が収集できること。
6	基本	セッション数が収集できること。
7	基本	実行待ちスレッド数が収集できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	AP サーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.7.インターネットサービス性能監視

インターネットサービス性能監視は、インターネットプロトコルで提供されるサービスに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	Web ページ【HTTP、HTTPS 等】の応答時間を収集できること。
2	基本	Web ページでの一連の操作を記録し、トータルでの応答時間の収集ができること。
3	基本	上記の場合において、途中の一部操作の応答時間が収集できること。
4	基本	上記の場合において、ページの内容が正しいかどうかを判断する機能を有すること。
5	基本	メール【SMTP、POP3、IMAP4 等】の送受信における応答時間の収集ができること。
6	基本	アドレス解決【DHCP、DNS 等】における応答時間の収集ができること。
7	基本	任意の TCP ポートへの接続時間の収集ができること。
8	基本	任意のアプリケーションの応答時間を測定するプログラムを起動し、その結果を収集できること。
9	加点	管理サーバ及びエージェントの間の電文を収集できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	計測サーバがクラスタ化されている場合、管理エージェントはクラスタ上で動作可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

関連する技術	
ハイパーテキスト転送プロトコル	HTTP(Hyper Text Transfer Protocol) Web サーバとクライアント(Web ブラウザ等)がデータを送受信するのに使われるプロトコル。HTML 文書や、文書に関連付けられている画像、音声、動画等のファイルを、表現形式等の情報を含めてやり取りできる。IETF によって、HTTP/1.0 は RFC 1945 として、HTTP/1.1 は RFC 2616 として規格化されている。 HTTPS(Hyper Text Transfer Protocol Security) Web サーバとクライアント(Web ブラウザ等)がデータを送受信するのに使われるプロトコルである HTTP に、SSL によるデータの暗号化機能を付加したプロトコル。サーバとブラウザの間の通信を暗号化し、プライバシーにかかわる情報やクレジットカード番号等を安全にやり取りすることができる。主要な Web ブラウザ【Internet Explorer、Firefox、Safari 等】が対応していることから、Web における暗号化の事実上の標準となっている。SSL は Netscape Communications 社が提唱した暗号化プロトコルで、HTTP 以外に FTP や TELNET 等のプロトコルの暗号化にも使われる。
DHCP	DHCP(Dynamic Host Configuration Protocol) インターネットに一時的に接続するコンピュータに、IP アドレス等必要な情報を自動的に割り当てるプロトコル。DHCP サーバには、ゲートウェイサーバや DNS サーバの IP アドレスや、サブネットマスク、クライアントに割り当ててもよい IP アドレスの範囲等が設定されており、ダイヤルアップ等の手段を使ってアクセスしてきたコンピュータにこれらの情報を提供する。クライアントが通信を終えると自動的にアドレスを回収し、ほかのコンピュータに割り当てる。DHCP を使うとネットワークの設定に詳しくないユーザでも簡単にインターネットに接続することができ、また、ネットワーク管理者は多くのクライアントを容易に一元管理することができる。
ドメインネームシステム	DNS(Domain Name System) インターネット上のホスト名と IP アドレスを対応させるシステム。全世界の DNS サーバが協調して動作する分散型データベースである。IP アドレスをもとにホスト名を求めたり、その逆を求めたりすることができる。各 DNS サーバは自分の管理するドメインについての情報をもっており、世界で約 10 台運用されているルートサーバにドメイン名と自分のアドレスを登録しておく。リゾルバと呼ばれるクライアントプログラムは、調べたいドメイン名（又は IP アドレス)をまずルートサーバに照会し、そのドメインを管理する DNS サーバを調べ、その DNS サーバに情報を聞き出すことで変換を行う。インターネット上で運用されている DNS サーバのほとんどは、カリフォルニア大学バークリー校(UCB)で開発された BIND である。

5.9.1.8.ジョブ管理サーバ稼動管理

ジョブ管理サーバ稼動管理は、ジョブ管理サーバに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	ジョブの実行数の収集ができること。
2	基本	エラーになったジョブ数の収集ができること。
3	基本	滞留しているジョブ数の収集ができること。
4	基本	実行が遅延しているジョブ数の収集ができること。
5	基本	使用している DBMS の稼動情報が収集できること。
6	基本	ジョブの実行待ち時間が収集できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	ジョブ管理サーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.9.Web サーバ管理ソフト稼動管理

Web サーバ管理ソフト稼動管理は、Web サーバの管理ソフトに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	アクセス数の収集ができること。
2	基本	Not Found 数(*)の収集ができること。
3	基本	スループットの収集ができること。
4	基本	送受信データの転送速度の収集ができること。

(*) Not Found 数：指定した URL の Web ページが見つからなかった回数

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	Web サーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.10.業務アプリケーション稼動管理

業務アプリケーション稼動管理は、業務アプリケーションに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	応答時間が収集できること。応答タイムアウトも検知できること。
2	基本	ディスパッチャ待ち時間の収集ができること。
3	基本	DBMS への依頼時間が収集できること。
4	基本	ログインユーザ数が収集できること。
5	基本	ログの収集ができること。
6	基本	ワークプロセスの稼動情報が収集できること。

非機能要件(個別の要件がある場合のみ記述)		
可用性	基本	業務アプリケーションサーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.11.グループウェア稼動管理

グループウェア稼動管理は、グループウェアに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	メールの送受信に関する情報が収集できること。
2	基本	ネットワーク(データ送受信)に関する情報が収集できること。
3	基本	メールサーバのキュー情報が収集できること。
4	基本	使用しているデータベースのキャッシュヒット率やディスク容量等のファイル情報が収集できること。
5	基本	グループウェアサービスの状態が監視できること。

非機能要件(個別の要件がある場合のみ記述)		
可用性	基本	グループウェアサーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

5.9.1.12.分散トランザクション稼動管理

分散トランザクション稼動管理は、分散トランザクションに関する稼動性能情報を収集する機能である。

機能要件		
1	基本	RPC(Remote Procedure Call)に関する性能情報を収集できること。
2	基本	ファイルアクセス回数を収集できること。
3	基本	コミット/ロールバック回数が収集できること。
4	基本	分散トランザクションサーバの通信状態が収集できること。
5	基本	キューマネージャーの稼動情報を収集できること。
6	基本	ハンドルの状況を収集できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	分散トランザクションサーバがクラスタ化されている場合、管理エージェントはすべてのサーバの管理が可能なこと。
拡張性	基本	収集したデータは必要に応じて外部記憶装置へ退避させ、必要なときに復旧できること。
拡張性	基本	収集データは、内部統制の監査に必要な期間分のデータ保存ができること。

関連する技術	
リモートプロシジャーコール	RPC（Remote Procedure Call） Sun Microsystems 社が開発した、ネットワーク上の異なるマシンで処理を実行する手続き。UNIX に広く普及し、現在では Windows NT にも実装されている。Microsoft 社の分散オブジェクト技術 DCOM は、この技術を基盤に開発された。

5.9.2.クライアント PC 管理の機能/非機能要件

5.9.2.1.クライアント PC 構成管理

クライアント PC 構成管理は、クライアント環境のハードウェア情報/ソフトウェア導入情報等を一括収集して管理するための機能である。不正クライアントのネットワーク接続、不正ソフトウェアの利用等を発見するためのセキュリティ機能としての役割ももつ。

機能要件		
1	基本	機器情報【CPU、メモリ、物理ディスク、MAC アドレス、外部記憶装置　等】が閲覧できること。
2	基本	各端末に導入されているソフトウェアの情報を収集できること。
3	基本	OS に関する情報【OS、バージョン、コンピュータ名、IP アドレス等のネットワーク情報　等】が閲覧できること。
4	基本	構成情報等は任意のタイミングで、グループ単位、ユーザ単位で収集できること。
5	基本	情報を収集する端末を選択できること。
6	基本	情報収集時には、利用者の作業を中断しないように GUI を表示しない、又は GUI を隠すことができること。
7	基本	収集した構成情報は一元管理し、閲覧及び条件検索ができること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	管理サーバがダウンしてもクライアント PC は利用できること。
パフォーマンス	基本	{数千}台の PC を同時管理できること。
拡張性	基本	分散サーバ等の活用により PC{数千}台まで拡大可能であること。
セキュリティ	基本	収集した PC 構成情報は適切な者のみアクセス可能とすること。

5.9.2.2.資源配布管理

資源配布管理は、サーバ側から一括で複数クライアントに対し、クライアントPC共通で利用する標準ソフトウェア、セキュリティパッチ等の配布(リモートインストール)を一括で実現するための管理機能である。

機能要件		
1	基本	サーバから端末へのソフトウェアの配布ができること。
2	基本	全端末への配布ができること。
3	基本	配布の実行時には、利用者の作業を中断しないようにGUIを表示しない、又はGUIを隠すことができるようにすること。
4	基本	配布終了時に再起動が必要な場合は、作業している利用者に再起動を促すメッセージを表示できること。
5	基本	【msi、exe　等】の主要インストーラの形式でのセットアップに対応可能であること。
6	基本	端末及びグループ単位で、インストール又はアンインストール可能なソフトウェアを定義できること。
7	基本	特定の端末及びグループに対して配布ができること。
8	基本	ソフトウェアの配布された結果を確認できること。
9	基本	電源OFFの状態から端末を起動して、ソフトウェア配布を行った後、自動的に電源OFFできること。
10	基本	資源配布にかかわる作業(インストールから再起動までのユーザ操作)が自動化でき、スケジュールにより資源配布できること。
11	基本	サービスパック等の大容量の資源配布において、業務に支障を与えないよう資源配布できること。
12	基本	資源配布実行後、正常に配布できなかったクライアント PC が特定でき、再度配布できること。
13	基本	サイレントモードでのインストールができないソフトウェアのインストール、バージョンアップが、利用者の操作なしに可能なこと。なお、特定の端末でインストール操作を行い、その際の変更記録をもとに配布ができれば、要件を満たしているものとする。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	基本	{数十万}台のPCを同時管理できること。
拡張性	基本	分散サーバ等の活用によりで{数十万}台まで拡大可能であること。
セキュリティ	基本	権限があるもの以外は配布操作及び配布資源の参照ができないこと。

5.9.2.3.遠隔操作

遠隔操作は、クライアント PC に対して、サーバ側からリモートでクライアント操作を実現するための管理機能である。

機能要件		
1	基本	管理者から特定のクライアント PC に対しリモートで接続でき、画面が表示できること。
2	基本	リモートから接続できる権限をもつ利用者を限定できること。
3	基本	リモート接続し、接続した端末にファイル転送ができること。
4	基本	リモート接続し、接続した端末の再起動ができること。
5	基本	対象のクライアント PC がログインしていない状態からリモート操作できること。
6	基本	リモート操作の通信内容は暗号化して送受信でき、操作内容を記録できること。
7	基本	操作対象端末の状態を変更する操作【ログオン、シャットダウン、再起動 等】はログ情報として記録可能なこと。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	基本	回線速度に応じて回線負荷(必要とされる帯域幅)を減らし、ネットワークを介した操作が可能なこと。

5.9.2.4.その他

機能要件		
1	基本	クライアント PC に関する操作ログが記録され、参照可能であること。操作ログとしては、少なくともプログラムの起動、ファイル操作を含むこと。

5.9.3.サーバ管理の機能/非機能要件

5.9.3.1.サーバ構成管理

サーバ構成管理は、サーバを構成するハードウェア情報及びソフトウェア情報を管理する機能である。

機能要件		
1	基本	サーバの構成情報として、すべてのサーバを対象に、デバイス情報、システム情報【OS、CPU、メモリ 等】、ソフトウェア情報、ネットワーク情報、ディスク情報の最新状態が集中管理できること。
2	加点	サーバの構成情報の変更履歴、変更前後の差分を表示できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	管理サーバがダウンしても管理サーバを操作する端末(コンソール端末)ではサーバ構成管理以外の利用ができること。
パフォーマンス	基本	{数百}台のサーバを同時に管理できること。
拡張性	基本	サーバ{数百}台まで拡大可能であること。
セキュリティ	基本	収集したサーバ構成情報(デバイス情報、システム情報、ソフトウェア情報、ネットワーク情報、ディスク情報等)はそれぞれ適切なアクセスが可能であること。

5.9.3.2.パフォーマンス管理

パフォーマンス管理は、サーバに要求されるレベルのパフォーマンスを監視するための管理機能である。

機能要件		
1	基本	各 OS のカーネルの設定情報を収集できること。
2	基本	IO、メモリ、キャッシュ、スペース、デッドロック、SQL 回数等のデータベースの性能情報を収集可能なこと。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	パフォーマンス管理機能は自機能不具合時に、他の業務(機能)に影響を与えずに容易に再起動できること。
拡張性	基本	パフォーマンス管理対象として、複数のデータベース、OS に対応すること。
拡張性	基本	パフォーマンス管理対象としてのデータベース、OS の新バージョンにも柔軟に対応できること。

5.9.3.3.障害管理

障害管理は、サーバにおける障害検知や業務システムを構成するサーバの異常時対策に関する管理機能である。

機能要件		
1	基本	特定のログ情報の出力機能を監視し、特定のイベントを検知した場合、アラーム等を管理者に通知すること。
2	基本	監視対象端末の状態を変更する操作【シャットダウン、リブート 等】はログ情報として記録可能であること。
3	加点	サーバ上で、各種サービス・デーモン等が制御する通信ポート【HTTP/HTTPS、DNS、SMTP、任意ポート 等】に対して、ポーリング監視ができること。
4	基本	サーバに常駐している各種サービス、デーモン、プロセスの稼動状態監視が可能であること。
5	基本	所定のマシンルームに設置する全サーバを対象として、ハードウェア異常等が発生した場合に、職員、保守窓口及び運用担当者等にメール(携帯電話へのメールを含む)等で通知できるように構成すること。
6	基本	障害発生時に影響範囲を特定可能であること。
7	基本	障害情報の履歴管理が可能であること。

非機能要件（個別の要件がある場合のみ記述）		
拡張性	基本	障害管理対象として、複数のデータベース、OS に対応すること。

5.9.3.4.資源管理

資源管理は、サーバ上に配置されたハードディスクの使用・空き容量を表示・通知する管理機能である。

機能要件		
1	基本	全サーバのハードウェア上のディスク使用量、空き容量のグラフ表示及びファイル出力機能が利用できること。
2	基本	ディスクの使用量のしきい値監視機能及び担当者への自動通知機能が利用できること。

5.9.3.5.バックアップ管理

バックアップ管理は、災害、システム障害(人為ミスも含む)等によるデータ破壊に備えた管理機能である。

機能要件		
1	基本	オンラインバックアップに対応しているソフトウェアについては、オンラインバックアップができること。
2	基本	スケジュールによるバックアップができること。
3	基本	フルバックアップ及び差分バックアップができること。
4	基本	バックアップの運用状況(成否)が監視できること。
5	基本	ファイル、フォルダ、論理ボリューム、サーバの単位でリストアできること。
6	基本	バックアップを取得したサーバ以外のサーバからもリストア操作ができること。
7	基本	システム領域を復旧するためのバックアップメディアを作成できること。
8	加点	システム領域のリストアは、バックアップメディアから起動し、行えること。
9	基本	業務で使用するネットワークに負荷をかける恐れがある場合は、バックアップ専用セグメントを配置すること。
10	基本	バックアップのメディアの世代管理ができること。ライブラリ装置と連携し、指定した世代数メディアに保存すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	バックアップのためにサーバの停止や再起動が発生しないこと。
セキュリティ	基本	権限がある者以外はバックアップメディアを参照できないこと。

5.9.3.6.設備連携

設備連携は、システム運用に必要な関連設備の異常時に関する管理機能である。

機能要件		
1	基本	所定のマシンルームに関する空調機、電源設備、漏水・温度等の状況を監視し、異常発生時には通知する機能を有すること。
2	基本	異常が発生したマシンルームに設置された機器に対して、オペレータ又は管理者が正常終了作業を実施する際の支援機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	設備異常を検知したときに、サーバのシャットダウンを確実に指令できること。
拡張性	基本	設備異常を認知できるインタフェースを有すること。

5.9.3.7.資源配布管理

資源配布管理は、管理サーバ側から一括で複数サーバに対し、利用する標準ソフトウェア、セキュリティパッチ等の配布(リモートインストール)を一括で実現するための管理機能である。

機能要件		
1	基本	管理サーバから対象サーバへのソフトウェアの配布ができること。
2	加点	配布の実行時には、利用者の作業を中断しないようにGUIを表示しない、又はGUIを隠すことができるようにすること。
3	基本	配布終了時に再起動が必要な場合は、作業している利用者に再起動を促すメッセージを表示できること。
4	加点	主要インストーラの形式でのセットアップに対応可能であること。
5	基本	サーバ及びグループ単位で、インストール又はアンインストール可能なソフトウェアを定義できること。
6	基本	特定のサーバ及びグループに対して配布ができること。
7	基本	ソフトウェアの配布された結果を確認できること。
8	加点	資源配布にかかわる作業(インストールから再起動までのユーザ操作)が自動化でき、スケジュールにより資源配布できること。
9	基本	サービスパック等の大容量の資源配布において、業務に支障を与えないよう資源配布できること。
10	基本	資源配布実行後、正常に配布できなかったサーバが特定でき、再度配布できること。
11	加点	サイレントモードでのインストールができないソフトウェアのインストール、バージョンアップが、利用者の操作なしに可能なこと。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	基本	｛数百｝台のサーバを同時管理できること。
拡張性	基本	分散管理サーバ等の活用によりで｛数百｝台まで拡大可能であること。
セキュリティ	基本	権限があるもの以外は配布操作及び配布資源の参照ができないこと。

5.9.3.8.その他

機能要件		
1	基本	サーバに関する操作ログが記録され、参照可能であること。

5.9.4.ネットワーク管理の機能/非機能要件

5.9.4.1.ネットワーク構成管理

ネットワーク構成管理は、ネットワークを構成するネットワーク機器情報及びソフトウェア情報を管理する機能である。

機能要件		
1	基本	ネットワークマップをネットワーク構成情報から自動で生成できること。
2	基本	各ノードの任意の MIB 情報を自動取得できること。
3	基本	ネットワーク機器の設置及び設定情報を管理できること。
4	基本	ネットワーク機器の台数の管理ができること。
5	基本	ネットワーク構成情報が自動で取得でき、ネットワーク機器から構成情報の定期アップデートができること。
6	基本	ネットワークマップをカスタマイズして、拠点、フロアごとに階層化されたネットワークマップを作成できること。
7	基本	構成情報は GUI により閲覧できること。
8	加点	過去に行った構成変更が、変更前後の差分として表示できること。
9	基本	構成情報は、拠点、部署等の目的に応じた表示が可能なこと。
10	基本	表示画面ごとに別々の構成情報を表示できること。
11	加点	構成情報は VLAN 経路ごとの表示が可能なこと。
12	基本	トラブルが発生した機器及び回線状態の状況をアイコンの色の変化等で表示可能なこと。
13	基本	業務の処理量や負荷に対して、ネットワーク機器及びサーバの CPU、メモリ等のどこにボトルネックがあるか監視できること。
14	加点	運用管理サーバ機器の故障が発生しても運用監視が切り替え時間なく継続可能こと。
15	基本	オペレータや管理者の不用意な操作によるネットワークのトラブルを防止するため、操作制限できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	ネットワークがダウンしてもサーバやクライアント PC はネットワークを利用しない機能が利用できること。
パフォーマンス	基本	PC{数十万}台、サーバ{数百}台を同時に管理できること。
拡張性	基本	PC{数十万}台、サーバ{数百}台まで拡大可能であること。
セキュリティ	基本	収集した監視対象機器の構成情報は適切な者のみアクセス可能とすること。

関連する技術	
ネットワーク管理プロトコル	SNMP (Simple Network Management Protocol) TCP/IP ネットワークにおいて、ルータやコンピュータ、端末等、ネットワークに接続された通信機器をネットワーク経由で監視・制御するためのプロトコル。制御の対象となる機器は MIB と呼ばれる管理情報データベースをもっており、管理を行う機器は対象機器の MIB に基づいて適切な設定を行う。 (仕様) http://www.ietf.org/rfc/rfc2570.txt?number=2570 (リンク＆情報ポータル) http://www.simpleweb.org/
MIB	MIB(Management Information Base) SNMP で制御されている機器がもつ管理情報。RFC 1156 として規定されている MIB1 と、RFC 1213 で規定されている MIB2 があり、現在では MIB2 を使うのが一般的となっている。IETF によって、標準化がなされている。 (仕様) http://www.faqs.org/rfcs/rfc1213.html

5.9.4.2.トラフィック管理

トラフィック管理は、ネットワークのトラフィックを管理する機能である。

機能要件		
1	基本	リアルタイムに、トラフィックが計測・収集できること。
2	基本	計測したトラフィック情報にしきい値を設定し、しきい値を越えた場合に担当者に自動通知できること。
3	基本	ネットワーク上において、通過するトラフィックを監視し、ユーザが定義したポリシーに従って、帯域や伝送遅延をコントロールし、きめ細かい帯域管理が行えること。ネットワーク上の監視・管理実施場所については別途示す。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	トラフィック管理機能が動作していても、動作していないときと同じように業務が利用できること。

5.9.4.3.障害管理

障害管理は、ネットワークの障害を管理する機能である。

機能要件		
1	基本	ネットワーク機器のノードダウン・リンクダウン監視、ICMP-echo を用いたノードステータス監視ができること。
2	基本	監視イベントの自動通知機能とフィルタリング機能が利用できること。
3	加点	フィルタリングによる監視イベント自動分類機能が利用できること。
4	基本	センターノードスイッチ及びローカルノードスイッチにおける接続ポートの強制的なリンクダウンがリモートでできること。
5	基本	リモートでの電源 ON・OFF・再起動が可能なネットワーク機器については、外部拠点にあるネットワーク機器類の電源 ON・OFF・再起動が一元的にできること。
6	基本	ネットワーク障害時に(ただし、当該ネットワーク機器への通信は可能な場合には)、ネットワーク機器の遠隔操作が可能なこと。
7	基本	障害の履歴管理が可能であり、履歴をキーワードで検索できること。

非機能要件（個別の要件がある場合のみ記述）		
拡張性	加点	データ保存として各種データベース、OS に対応していること。
可用性	基本	通知方法が複数用意されていること【パトランプ、メール　等】。また、監視を多重化して管理サーバに通知できること。
可用性	加点	ネットワーク機器が出力する Syslog の監視及び蓄積管理を行えること。

5.9.4.4.その他

機能要件		
1	加点	ネットワーク管理に関する操作ログが記録され、参照可能であること。

5.9.5.ストレージ管理の機能/非機能要件

5.9.5.1.ストレージ構成管理

ストレージ構成管理は、ストレージ装置の属性や論理ディスク構成、接続状況等を表示・通知する機能である。

機能要件		
1	基本	ストレージの構成情報収集機能が利用できること。
2	基本	接続されているストレージ機器の自動検知機能が利用できること。
3	基本	接続されているストレージ機器のマップ作成機能が利用できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	ストレージがダウンしてもストレージ管理サーバやストレージに接続されているサーバやクライアント PC は継続して利用できること。
セキュリティ	基本	収集したストレージ構成情報は適切な者のみアクセス可能とすること。

5.9.5.2.性能管理

性能管理は、性能状況をリアルタイムに表示・監視し、未然に性能劣化を検知するための機能である。

機能要件		
1	基本	ストレージ装置の Read/Write の回数、データ転送、平均応答時間、ディスク使用率といった性能情報を取得し、監視できること。
2	基本	サーバとストレージ間の性能情報【SAN スイッチの性能情報　等】を取得し、監視できること。
3	基本	ストレージ装置の性能情報及びサーバとストレージ間の性能情報に対するしきい値監視機能及び担当者への自動通知機能が利用できること。
4	基本	性能情報のグラフ表示及びファイル出力機能が利用できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	性能管理機能がダウンしてもストレージ装置の継続稼動ができること。

5.9.5.3.資源(容量)管理

資源(容量)管理は、ディスク単体や論理グループごとでの使用・空き容量を表示・通知するための機能である。

機能要件		
1	基本	ストレージに接続された各サーバの資源(容量)情報の収集・保存ができること(デバイス、ボリューム、サーバそれぞれにおける使用量、空き容量が把握できること)。
2	基本	使用量のしきい値監視機能及び担当者への自動通知機能が利用できること。
3	基本	グラフ表示及びファイル出力機能が利用できること。
4	加点	フォルダ、ユーザ単位で使用量、空き容量が把握できること。
5	基本	使用量に基づき部署別等の課金額を計算する機能を有すること。
6	基本	増設したディスクにも対応できること。

非機能要件(個別の要件がある場合のみ記述)		
パフォーマンス	基本	資源(容量)管理機能によりストレージ装置の性能に影響を与えないこと。

5.9.5.4.障害管理

障害管理は、ストレージ装置を監視し、その状態表示や障害発生時のメッセージを出力する機能である。

機能要件		
1	基本	監視イベントの自動通知が利用できること。
2	基本	フィルタリング機能が利用でき、かつフィルタリングによる監視イベント自動分類機能が利用できること。
3	加点	ストレージ障害時にストレージ機器の遠隔操作ができること(電源 ON/OFF/再起動の一元管理)。
4	基本	操作ログ/コンソールログ、イベントログ、コンフィグ等が収集できること。
5	基本	メンテナンスに入るまでの段階的な切断を行う等への対応のため、SAN スイッチにおける接続ポートの強制的なリンクダウンがリモートでできること。

非機能要件(個別の要件がある場合のみ記述)		
拡張性	基本	各種データベース、OS に対応していること。
可用性	基本	通知方法が複数用意されていること【パトランプ、メール　等】。また、監視を多重化して管理サーバに通知できること。

5.9.5.5.バックアップ管理

バックアップ管理は、災害、ストレージ障害(人為ミスも含む)等によるデータ破壊に備えた機能である。

機能要件		
1	基本	LAN フリーバックアップ又はサーバレスバックアップを行うことができる機能を有していること(*)。
2	基本	拠点間でのリモートバックアップ、ディザスタリカバリ等に利用できる機能を有していること。

(*)LAN フリーバックアップ:LAN を経由せず、SAN 経由でデータをバックアップする方式。
　サーバレスバックアップ:LAN を経由せず、さらにサーバにも負担をかけないバックアップ方式。

非機能要件（個別の要件がある場合のみ記述）		
セキュリティ	基本	権限がある者以外はバックアップメディアを参照できないこと。

5.9.5.6.その他

機能要件		
1	基本	ストレージに関する操作が記録され、参照可能であること。

5.9.6.サービスデスクの機能/非機能要件

5.9.6.1.サービスデスク管理

サービスデスク管理は、情報システムのトラブルや使用方法等の問い合わせを一括して受け付け、管理する機能である。

機能要件		
1	基本	メール及び GUI による問い合わせが管理できること。
2	基本	問い合わせを自動的に担当者に通知し、登録でき、データベースとして蓄積できること。
3	基本	トラブルチケットや問題票や変更管理の帳票等に、補助情報としてファイルを添付できること。
4	基本	過去に問い合わせをした内容を GUI により閲覧、検索できること。
5	基本	エスカレーション機能が利用できること。
6	基本	ほかの管理機能において障害情報を検知した場合、連携による自動登録できること。
7	基本	情報システム関連の申請窓口をサービスデスクに統合できること。

非機能要件（個別の要件がある場合のみ記述）		
拡張性	加点	サーバ監視、ネットワーク監視と連携できるインタフェースを有すること。
可用性	基本	管理する問い合わせの数にプログラム的な上限を設けないこと(拡大可能なこと)。

5.9.6.2.その他

機能要件		
1	基本	サービスデスクに関する操作が記録され、参照可能であること。

5.9.7.セキュリティの機能/非機能要件

5.9.7.1.ウイルス対策機能

ウイルス対策機能は、不正なプログラムがサーバや端末(PC)に不正プログラムが感染することを防止するために、感染した不正プログラムを検出する機能である。

機能要件		
1	基本	ウイルスソフトウェア及びワクチンソフトウェアは提案する OS に適合すること。
2	基本	ウイルスチェックする時間は、スケジュールを設定して自動的に実行できること。ウイルスチェック実行時に利用者が PC をシャットダウンしようとする場合、ウイルスチェック終了時に自動的に PC をシャットダウンするか、又は PC の次回起動時に再実行できること。
3	基本	ウイルス定義のパターンファイルは、スケジュールを設定してパターンファイル納入元のサーバにインターネット等を経由してアクセスし、自動的に更新できること。
4	加点	ウイルス定義のパターンファイル更新時にはシステムを再起動せずに更新できること。
5	基本	感染した不正プログラムをリアルタイムで検出し、不正プログラムの隔離又はウイルスの駆除ができること。
6	基本	パターンファイルはサーバにて一元管理して、端末に配布できる機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	ワクチンソフトウェアの異常でサーバや端末(PC)を停止しないこと。
可用性	基本	ウイルス定義のパターンファイル等の配布サーバ停止により、検出機能が停止しないこと。
可用性	基本	ウイルスチェックに使用する最新のパターンファイルが配布されること。
セキュリティ	基本	偽装したウイルス定義のパターンファイルの配布ができないこと。
セキュリティ	基本	ワクチンソフトウェアの停止及びアンインストールをエンドユーザができないこと。
パフォーマンス	加点	ウイルスチェック時やパターンファイル配布時に通常の動作プログラムを著しく遅延しないこと。
拡張性	基本	ウイルス定義のパターンファイル等の配布対象が増えたときにスケーラブルに対応できること。

・政府機関統一基準に対応する項目：２．１．１．４、２．１．２

・物理構成モデルのセグメントに対する項目：S0、S1

5.9.7.2.インターネットコンテンツフィルタリング機能

インターネットコンテンツフィルタリング機能は、Web(インターネット)上の有害情報へのアクセスを遮断する機能である。

機能要件		
1	基本	保護対象の内部ネットワークから、インターネットの特定 URL に対するアクセス制限機能を導入すること。
2	基本	禁止 URL のデータベースは、PICS 等のデータベース提供元のサーバにインターネット経由でアクセスし、自動的に更新できること。
3	基本	禁止 URL のデータベースの更新チェック間隔を指定できること。
4	基本	特定の利用者のみに URL を許可する設定が可能なこと。
5	基本	禁止 URL へのアクセスが監視できること。
6	基本	海外及び国内の十分な禁止 URL データをもつこと。
7	基本	禁止 URL 及び許可 URL をカテゴリ別に詳細に設定できること。
8	基本	部署ごと・ユーザごとに異なるフィルタリングポリシーを適用可能なこと。
9	基本	ディレクトリサービスと連携し、一元的なユーザ管理が可能なこと。
10	基本	複数サーバによる負荷分散環境においても、一つのルール設定を実施することで複数のサーバに同期が可能なこと。
11	基本	「閲覧は許可するが情報送信はできない」「書き込み内容を見てフィルタリング」といった柔軟な設定が可能なこと。
12	基本	カテゴリごと、ユーザごとのアクセス状況をグラフ化して表示可能なこと。
13	基本	アクセスログから、【ユーザ名、グループ名、ブロック状況　等】の必要な情報を抽出可能なこと。
14	基本	検索エンジンのキャッシュや翻訳サイトの翻訳機能に対してもフィルタ可能なこと。ブロックログ・POST ログは管理画面もしくはレポートソフトから閲覧可能なこと。
15	加点	Web コンテンツを解析してウイルス検出する機能を有すること。
16	加点	ICAP クライアント機能又はきょう体内にて、同等の機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	コンテンツフィルタリング機能の異常でサーバや端末(PC)を停止しないこと。
可用性	基本	コンテンツフィルタリングのパターンファイル等の配布サーバ停止により、検出機能が停止しないこと。
可用性	基本	コンテンツフィルタリング機能に障害があった場合でも、エンドユーザに設定変更等を求めることなく、ネットワーク通信が継続的に阻害されないこと。
セキュリティ	基本	正規のパターンファイルであることを確認できるよう、サーバ証明書等でパターンファイルの配布元サイトを確認する手段を設けること。
セキュリティ	基本	コンテンツフィルタリング機能の停止及びアンインストールをエンドユーザができないこと。
パフォーマンス	基本	コンテンツフィルタリング時やパターンファイル配布時に通常の動作プログラムを著しく遅延しないこと。
拡張性	基本	コンテンツフィルタリングの対象となる端末が増えたときにスケーラブルに対応できること。

関連する技術	
コンテンツ制限規格	PICS (Platform for Internet Content Selection) Web コンテンツをユーザが設定するレベルに合わせて、選択的に受信する機能を実現するための技術仕様。W3C によって規格が制定されている。 （規格） http://www.w3.org/PICS/

・政府機関統一基準に対応する項目：2．1．1．2、2．1．1．4、2．2．3．2

・物理構成モデルのセグメントに対する項目：S1

5.9.7.3.スパムメール対策機能

スパムメール対策機能は、メール受信者の意向を無視して一方的に送信されるメッセージ(スパムメール)を遮断する機能である。

機能要件		
1	加点	クライアントマシンからスパムメール発信を抑止する、パーソナルファイアウォール機能を有すること。
2	基本	ホームページ等で外部に公開しているメールアドレスについては、職員用のメールアドレス等と比較して、情報セキュリティの脅威にさらされる可能性が高いため、(サーバを分離する等の)相応の対処を施すこと。
3	基本	スパムメールの受信が監視できること。
4	基本	送信元の IP アドレスによりスパムメールをブロックが可能なこと。
5	基本	送信者が明らかなスパムメールをブロック可能なこと。
6	基本	ホワイトリストにより、ブロックせずにメッセージ転送が可能なこと。
7	基本	詐欺/悪質サイトの URL が記載されているスパムメールをブロックが可能なこと。
8	基本	スパム用フィンガープリントもしくは、それと同等以上のセキュリティレベルを保つルールセット等にて、ブロックが可能なこと。
9	基本	スパムと判断したメールに対し、隔離、タグ付け配信、破棄等の設定が可能なこと。
10	基本	統計的にスパムの状況が確認可能なこと。
11	加点	スパムメール抑止には、アプライアンス又はソフトウェアで提供できること。
12	加点	配信側のドメイン対策として、OP25B,DKIM、SPF 等インターネットに SPAM メールが配信されないような機構を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	スパムメール対策機能の異常でサーバや端末(PC)を停止しないこと。
可用性	基本	スパムメール対策のパターンファイル等の配布サーバ停止により、スパムメール対策機能が停止しないこと。
可用性	基本	機能又はスパムメール対策用のサーバが停止した場合でも、メール送受信等に悪影響が及ばないような措置を講ずること。
セキュリティ	基本	偽装したスパムメール対策のパターンファイルの配布ができないこと。
セキュリティ	基本	スパムメール対策機能の停止及びアンインストールをエンドユーザができないこと。
パフォーマンス	基本	スパムメールチェック時やパターンファイル配布時に通常の動作プログラムを著しく遅延しないこと。
拡張性	基本	スパムメール対策のパターンファイル等の配布対象が増えたときにスケーラブルに対応できること。
パフォーマンス	加点	多量なスパムメールを受信しても処理できること。

・政府機関統一基準に対応する項目：２．２．３．１

・物理構成モデルのセグメントに対する項目：S0、S1、S2、S3、S5

5.9.7.4.ファイアウォール機能

ファイアウォール機能は、特定のネットワークとその外部のネットワーク間の通信を制御することにより、特定のネットワークの安全を確保する機能である。

機能要件		
1	基本	インターネット、内部ネットワーク、及び利用システムの接続点には、ファイアウォール機能を有する機器を接続し、特定の通信のみを許可すること。
2	基本	IP アドレスやポート番号を見て通過の可否を決めるパケットフィルタリング機能を有すること。
3	基本	IPv4 及び IPv6 の両方のプロトコルに対応していること。
4	基本	管理者がファイアウォールで通過が拒否されたアドレス情報等の監査情報を設定できること、また監査情報の設定と確認は遠隔でも利用できること。
5	基本	通信フローを見てパケットの通過の可否を決めるステートフルインスペクション機能を利用できること。
6	基本	TCP ポート番号変換機能(NAPT)を有すること。
7	基本	アドレス変換機能(NAT)を有すること。
8	基本	UDP 通信の監視もできるように、IP アドレス、ポート番号の組み合わせに対してタイマによる通過制御ができる機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	複数台による冗長構成とし、障害発生により一つのファイアウォール機能が停止しても、運用を継続できること。
パフォーマンス	基本	多量のパケットを受信したときに通常の処理が続けられること。
セキュリティ	基本	IDS と連携して不信なパケットを拒否する機能を有すること。

・政府機関統一基準に対応する項目：2.1.1.2,2.1.1.4,2.1.2.3,2.2.4.1

・物理構成モデルのセグメントに対する項目：S1

5.9.7.5.侵入検知・防止機能

侵入検知機能は、ネットワーク上の通信を監視し、不正なアクセスの兆候を検知する機能である。

機能要件		
1	基本	ネットワーク型 IDS(Intrusion Detection System)でネットワークを流れるパケットを解析してファイアウォールで防げない攻撃を検知する機能を有すること。
2	基本	IPv4 及び IPv6 の両方のプロトコルに対応していること。
3	基本	パターンファイルは、スケジュールを設定してパターンファイル納入元のサーバにインターネット等を経由してアクセスし、自動的に更新できること。
4	基本	侵入を検知したら、ファイアウォール等の関連する機器、ソフトと連携して当該セグメント、ホストへの不正な通信を遮断するとともに、関連するログの出力、監視装置への警報を行う機能を有すること。
5	基本	侵入防止のために IDS と連携したファイアウォールや IPS 機能で不正なパケットの侵入を防ぐ機能を有すること。
6	基本	信頼性の高いパターンファイルが随時提供されるシグネチャー型、アノマリー型の検出機構を有すること。
7	加点	アプリケーション攻撃(SQL インジェクション、クロスサイトスクリプティング等)を防止する機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	インラインで設置する場合、機器の障害が発生した場合にもネットワークが切断することがないよう、パススルー(バイパス)するための回路をもっていること。
可用性	基本	ログの増加により機能停止しないこと。
セキュリティ	基本	ネットワーク型 IDS はステルスモードで動作ができること。

・政府機関統一基準に対応する項目：1.5.1.1,2.1.1.4,2.2.4.2

・物理構成モデルのセグメントに対する項目：S1

5.9.7.6.ネットワーク接続監視機能

ネットワーク接続監視機能は、保護対象となる特定のネットワークに対して、脅威となる端末(PC)の接続を制御する機能である。

機能要件		
1	基本	端末等が保護対象のネットワークに接続する前にセキュリティに関する検査を行い、不合格の場合はネットワーク機器と連携して検疫(ネットワークからの隔離)を行う機能を有すること。
2	基本	未承認の端末等がネットワークに接続された場合に、その端末等を監視画面上の特定のエリアに表示する、又はメッセージを表示する等により、検知する仕組みを導入すること。
3	基本	セキュリティ検査に不合格の場合はネットワークからの隔離(検疫)を行い、セキュリティ更新のためのアップデート専用サーバの利用のみを許可する機能を有すること。
4	基本	端末のセキュリティの適合状態をチェックするソフトウェア等により、検疫ネットワークが実現できること。
5	基本	端末の不正接続防止機能【IP アドレスや MAC アドレスによる認証機能、IEEE802.1x 認証機能　等】を有すること。
6	基本	OS のセキュリティパッチ適用状況、OS のファイアウォール設定状況、スクリーンセーバ及びログインパスワードの設定状況、ウイルス対策ソフトの導入状況、ウイルス対策ソフトのパターン更新状況、ウイルス対策ソフトのリアルタイムスキャンの設定状況、任意に設定したソフトの導入状況の検査及び、検疫結果不合格な端末の隔離、検疫結果不合格な端末の管理者への警告が行えること。
7	基本	指定期間中の接続端末数や端末別のセキュリティ状況等を集計し、テキストフォーマットのファイル形式で出力する機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	ネットワーク接続監視機能の冗長化を図り、ネットワーク接続監視機能を装備したネットワーク機器(サーバ)に障害が発生しても運用を継続できること。
可用性	基本	ネットワーク接続監視機能が、何らかのトラブルを生じた場合、その機能を容易にネットワークから切り離し又は停止できること。すなわち、ネットワーク接続監視機能によってネットワークへ正当な権限を有する PC が一切接続しないという類の状況が発生してはならないこと。
拡張性	基本	複数台の端末を接続可能なこと。

関連する技術	
IEEE802.1x 認証	Institute of Electrical and Electronic Engineers 802 シリーズ IEEE(米国電気電子学会)で LAN 技術の標準を策定している 802 委員会が定めたアクセスポイントのユーザ認証を定める規格。 （仕様） http://www.ieee802.org/1/pages/802.1x.html

・政府機関統一基準に対応する項目：2.1.1.2,2.1.1.4,2.1.2.3,2.2.4.1

・物理構成モデルのセグメントに対する項目：S0、S1、S6

5.9.7.7.ウイルスゲートウェイ

ウイルスゲートウェイは、ネットワークパフォーマンスを低下させることなく、e-mail(SMTP、POP3、IMAP)、転送ファイル(FTP)、Web(HTTP)トラフィックからのウイルスやワーム、スパイウェア等に対してネットワークを防御する機能、及び添付ファイルに対してスキャンを行う機能である。

機能要件		
1	基本	最新ウイルスのパターンファイルを自動的にダウンロードし、更新可能なこと。
2	基本	ウイルスのパターンファイルがアップデートされた場合、提供元から即時に「プッシュ」アップデート可能な機能、あるいは管理者が即時に「プル」アップデート可能な機能を有すること。
3	加点	ウイルスを確認するポート(管理用ポートを除く)は、IP アドレスを割り振る必要なく、ブリッジで接続できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	ウイルスチェックに使用するパターンファイルは、ウイルスの検体が発見されてから「24」時間以内に配布されること。

・政府機関統一基準に対応する項目：2.1.2.2,2.4.3

・物理構成モデルのセグメントに対する項目：S1、S2

5.9.7.8.VPN 暗号化機能

VPN(IPSecVPN、SSL-VPN、等)は、通信路を暗号化する機能である。

機能要件		
1	基本	行政情報システム関係課長連絡会議(平成 15 年 2 月 28 日)の「各府省の情報システム調達における暗号の利用方針」に記載された暗号を用いているものであること。
2	基本	暗号化に用いる暗号鍵として、グループごと、情報共有相手ごとといった複数の暗号鍵を設定できること。
3	基本	暗号化・復号の操作をせずに暗号化通信できること。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	基本	通常の業務が著しく遅延しないこと。

関連する技術	
標準暗号化方式	AES(Advanced Encryption Standard) 米国商務省標準技術局(NIST)によって選定された、米国政府の次世代標準暗号化方式。1977 に制定された DES の安全性が低下したため、FIPS PUB197 として 2001 年 3 月に制定された。 (FIPS PUB197) http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
標準暗号化方式	3DES(Triple - Data Encryption Standard) IBM 社が開発した暗号化方式。同社が開発した秘密鍵暗号方式である「DES」を三重に適用するようにしてよりセキュリティを高めている。
電子証明書	X.509 証明書 ITU-T が策定した公開鍵証明書の標準であり、X.500 ディレクトリシリーズの一つとして、ISO/IEC の国際標準に規定されている。 1997 年に発行された最新バージョン(X.509v3) においては、証明書に拡張領域が設けられ任意の拡張が可能になった。X.509v3 は、2000 年に改定され、失効情報を迅速に利用者に通知するための方法と属性証明書の定義が明確になった。

・政府機関統一基準に対応する項目：2.1.1.6,2.2.4.1,2.2.4.2,2.2.4.3

・物理構成モデルのセグメントに対する項目：S0

5.9.7.9.HTTPS 暗号化機能

HTTPS 暗号化機能とは、TLS 暗号化プロトコルと組み合わせることにより HTTP の通信の安全性を向上させるための機能をいう。

機能要件		
1	基本	インターネットに公開される HTTP サーバにおいて、特に閲覧の対象者を限定する必要がある場合や、HTTP サーバに対して利用者からのデータをアップロードする必要がある場合等、利用者とサーバ間の通信の改ざん、盗聴を防ぐ必要があると判断される場合に適用する。
2	基本	行政情報システム関係課長連絡会議(平成 15 年 2 月 28 日)の「各府省の情報システム調達における暗号の利用方針」に記載された暗号を用いているものであること。
3	基本	複数の異なる種類の Web ブラウザで利用可能なこと。
4	基本	特に重要なデータのアップロード等を行う場合には、SSL サーバ認証、SSL クライアント認証ができること。
5	基本	HTTPS の通信に関しては、認証及び認証後の通信の記録を取得し、一定期間保管すること。
6	基本	上記の保管は証跡管理機能で管理することで代替することを認める。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	基本	通常の業務が著しく遅延しないこと。
パフォーマンス	基本	特にアクセスが集中する HTTP サーバを TSL 化する場合には、TSL 化専用のサーバの導入を検討すること。
可用性	基本	TLS 化専用サーバを設置している場合、当該のサーバが障害等の理由により停止した場合においても、HTTP サーバに影響を与えないこと。

関連する技術	
セキュリティプロトコル	TLS(Transport Layer Security) セキュリティを必要とする通信において、暗号化の機能を提供するプロトコル。TCP 通信をラッピングする形で実現されているため、その上位のプロトコルには依存しない。 (TSL1.1/RFC4346)http://tools.ietf.org/html/rfc4346

・政府機関統一基準に対応する項目：1.3.1.1,1.3.1.2,1.3.1.3,2.1.1.4

・物理構成モデルのセグメントに対する項目：S0、S1

5.9.7.10.ファイル暗号化機能

ファイル暗号化機能は、ファイルを暗号化する機能である。

機能要件		
1	基本	暗号化機能の適用は、省内外で利用する端末に適用すること。
2	基本	ワードプロセッサソフトウェアや表計算ソフトウェアで作成した文書等のファイルを暗号化できること。
3	基本	行政情報システム関係課長連絡会議(平成 15 年 2 月 28 日)の「各府省の情報システム調達における暗号の利用方針」に記載された暗号を用いているものであること。
4	基本	部署やプロジェクトごとに、ファイルサーバ上で共有している情報を暗号化し、アクセス制限を設けることで、第 3 者が閲覧できないようにすること。
5	基本	簡易な操作で暗号化・復号化できること。
6	基本	ハードディスクを自動的に暗号化可能であること。
7	基本	外部媒体にファイルを格納する際に容易にファイルを暗号化できること。
8	基本	省内端末に接続した外部メディア(USB メモリ、MO、フロッピーディスク、外付け HDD 等)にデータを保存する際に暗号化しないと持ち出せないようにできること。
9	基本	省内端末に接続した外部メディア(USB メモリ、MO、フロッピーディスク、外付け HDD 等)にデータを保存する際にデータを自動に暗号化すること。
10	基本	省内から省外に暗号化したファイルを渡す場合には、省外の端末に特別な暗号化ソフトがインストールされていなくてもパスワード等を入力することで復号できること。

非機能要件（個別の要件がある場合のみ記述）		
パフォーマンス	基本	通常の業務が著しく遅延しないこと。
バックアップ	基本	暗号化を行った端末(PC)やサーバが何らかの理由で破損した場合でも、ファイルの復号を可能とするように、バックアップしておいた復号鍵等を使用して暗号化したファイルを復号できるような手段を講じておくこと。

・政府機関統一基準に対応する項目：2.1.1.6,2.2.4.1,2.2.4.2,2.2.4.3

・物理構成モデルのセグメントに対する項目：S0、S3、S6

5.9.7.11.証跡管理機能

証跡管理機能は、システムあるいはネットワークを利用するユーザ(プログラムを含む)のログインやログオフを始めとしたログを管理する機能である。

機能要件		
1	基本	クライアントPC 及びサーバにおけるメール送信、Web アクセス、ファイル操作、印刷履歴等のログを収集、保管する機能を有すること。
2	基本	ログの収集を行う前に、あらかじめ収集対象となる情報資産を設定できること。
3	基本	アクセス対象の情報資産名、アクセスしたユーザ名、情報資産に対する操作内容、アクセス日時を証跡として収集できること。
4	基本	ログは自動出力され一元管理できること。
5	基本	収集した証跡情報は統計的な分析を行い、グラフ等に結果を出力できる機能を有すること。
6	基本	ログを収集・長期保存・バックアップができ、必要に応じて閲覧できる機能を有すること。
7	基本	ログの検索・集計結果は、CSV 形式又は PDF 形式で出力する機能を有すること。
8	基本	ログの集計結果はグラフ化して出力する機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
セキュリティ	基本	収集後のログが改ざんされないこと。
セキュリティ	基本	証跡のログは、第三者に不正に利用されることがないように、アクセス制御、暗号化、改ざん防止、改ざん検出等の措置を講ずること。
拡張性	基本	OS ログ(システムやアプリケーションの正常／エラーログ)も対応できること。
パフォーマンス	基本	ログ収集時にログ出力機能を著しく遅延しないこと。
バックアップ	基本	証跡のログは、バックアップを取得する等、ファイルの破損、消去等から保護するための措置を講ずること。

・政府機関統一基準に対応する項目：1.3.1.1,1.3.1.2,1.3.1.3,2.1.1.4

・物理構成モデルのセグメントに対する項目：S0、S1、S2

5.9.8.ジョブ管理の機能/非機能要件

ジョブ管理機能は、定型業務等決められた手順を流れに沿って定義し、日・時・イベント等を契機にジョブを実行する機能である。

機能要件		
1	基本	システム運用カレンダの定義が可能であること。
2	基本	システム運用カレンダに従ってプログラム・ジョブ実行がスケジューリングでき、自動実行が可能であること。
3	基本	ジョブ運行制御の一元管理が可能であること。
4	基本	ジョブの実行状況、実行履歴はログ情報として記録可能であること。
5	基本	ジョブの実行状況がモニタリング可能であること。
6	加点	イベント【タイマ、ファイル受信、ファイル変更　等】を契機にジョブの実行が可能であること。
7	基本	1 日を{48}時間で管理できること。
8	加点	大量ジョブの一括定義・変更ができること。

非機能要件（個別の要件がある場合のみ記述）		
セキュリティ	加点	利用者の権限に応じて使える機能【定義・実行・参照　等】に制限がかけられること。
バックアップ	基本	カレンダ定義・ジョブ定義のバックアップが行えること。

5.9.9.仮想化への対応

機能要件（仮想化環境への対応）		
1	基本	仮想化機構により実現された仮想化ゲストサーバ、仮想化ストレージ、仮想化ネットワークなどから構成される仮想化環境において物理サーバ環境と同等のソフトウェアを配置でき、同等の機能を満たすことができること。

5.10.EIP

5.10.1.定義

EIP(Enterprise Information Portal)は、IT システムを使った業務を効率的に実施するために有益な情報やアプリケーション群を一元的に集約して端末上の Web ブラウザに配信する機能を有した企業情報ポータルである。ポータルサイト利用者の役割に応じて適切なコンテンツやアプリケーションを関連付けたビュー(画面)を提供する。

EIP の機能・サービス	
機能・サービス	定義
ポータルサイト機能	複数のアプリケーション(業務アプリケーション、グループウェアアプリケーション)群、情報コンテンツ(文書、画像、動画等)を統合したビューを生成して、Web ページ(ポータルサイト)の形で Web ブラウザに送信し、また Web ブラウザからの入力を受信する機能。
パーソナライズ機能	ポータルサイト利用者を特定し、その利用者や利用者の役割ごとに適したコンテンツやアプリケーションの組み合わせを生成して、それを一元化した画面/ビューとして提供する機能。
アプリケーション統合機能	ポータルサイトの利用者の業務役割とアプリケーション群とを関連付けて、ポータルサイト上で統合し互いに連携させるための仕組み。対象となるアプリケーションとしてはグループウェア、知的情報活用(BI)、顧客関係管理(CRM)、企業資源計画(ERP)等の業務パッケージに加えて XML Web サービスのアプリケーションが挙げられる。
管理	EIP に関する管理機能。ユーザ管理、コンテンツ管理、監査、各種管理機能、バックアップ等。

5.10.2.ポータルサイト機能

機能要件		
1	基本	ポータルサイトごとに利用者の認証/認可を行えること。またサーバ外部のディレクトリサービスと連携した認証・認可を行えること。
2	基本	カスタマイズ:ポータルサイトに含める情報コンテンツやアプリケーションの組み合わせ、画面配置レイアウトを自由に変更できること。
3	基本	検索:ポータルサイト画面上に配置された検索フィールドや検索アプリケーションに検索キーワードを入力して、そのキーワードでポータルサイト上の情報コンテンツ群やアプリケーションのデータ検索を行い、その検索結果の情報を同サイト画面に表示する機能を有すること。
4	基本	ポータルサイトは機器【パーソナルコンピュータ、PDA、携帯電話　等】上の Web ブラウザからのアクセスにも応答できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	基本	ポータルサイトは複数のサーバハードウェア上で多重化させ、単一のサーバが障害になっても他方のサーバでシステムを継続動作させせることができる構成を有すること。
負荷分散	基本	ポータルサイトのサーバは複数のサーバハードウェアに多重化させ、サイトへのアクセス要求の負荷を分散させることができる構成を有すること。
性能	基本	ポータルサイトへの同時アクセスユーザ数の要求量を十分に処理できる性能を有すること。

関連する技術	
ディレクトリサービスプロトコル	LDAP (Lightweight Directory Access Protocol)

5.10.3.パーソナライズ機能

機能要件		
1	基本	カスタマイズ機能：利用者の業務の役割に応じて、必要となるコンテンツ情報やアプリケーションの組み合わせ、画面配置レイアウトを定義・編集することが可能であること。
2	基本	パーソナライズ機能：ログオンしたユーザの属性情報により、見せたい情報やアプリケーションを変更することが可能であること。

5.10.4.アプリケーション統合機能

機能要件		
1	基本	ポートレット連携：自サーバ内のポートレットや、ほかのサーバ上のアプリケーション機能やコンテンツを操作するために Web サービスとして公開されるリモートポートレットを連携・統合できること。
2	基本	外部接続：ネットワークでつながれた、共通基盤内/外で稼動する業務システム、業務アプリケーション、データベースと連携できること。
3	基本	Web サービス連携：Web サービスで提供しているアプリケーションと連携してポータルサイトの画面での統合/連携ができること。
4	基本	以下のようなグループウェアアプリケーション群をポータルサイトの画面で統合ができる機能を有すること。 ①スケジュール機能 ②会議室、掲示板 ③電子メール ④定型業務ワークフロー【勤怠管理、経費精算等】 ⑤データベース検索 ⑥文書管理
5	加点	アプリケーション連携：アプリケーションパッケージ製品【知的情報活用(BI)、顧客関係管理(CRM)、企業資源計画(ERP)等】と連携してポータルサイトの画面で統合/連携できる機能を有すること。

関連する技術	
Web サービス関連プロトコル	SOAP WSDL

5.10.5.管理

機能要件		
1	基本	ユーザ管理：ポータルサイトにアクセスできるユーザの ID、個人情報を管理(登録/編集/削除)できること。
2	基本	監査：ポータルサイト内のコンテンツやアプリケーションへのアクセスの履歴(ログ)を閲覧できること。またアクセス履歴の情報には、日時、アクセスしたコンピュータを特定する情報、アクセスの結果(成功/拒否)等の情報が含まれること。
3	加点	シングルサインオン：利用者がポータルサイトにログインする際の利用者 ID やパスワードと、コンテンツやアプリケーションの認証/認可に必要となる利用者 ID やパスワードとを関連付けて管理し、利用者はポータルサイトにログインする際に 1 回だけ利用者 ID とパスワードを入力すれば、アクセスするコンテンツ/アプリケーションへの認証/承認が自動的に行われる機能を有すること。

非機能要件（個別の要件がある場合のみ記述）		
バックアップ	加点	ポータルサイト上の情報コンテンツや管理データをバックアップすることのできる構成を有すること。

5.11.公開 Web サーバ

5.11.1.定義

インターネットを通して情報コンテンツの配信を行うWebサーバ。主に国民・企業等への情報公開での利用を想定している。24 時間×7 日間/週、多様な場所、不特定のクライアントからアクセスされうることから、悪意をもった様々な攻撃(データ改ざん、サービス妨害、情報漏えい、アクセス権限の不正昇格、否認等)を受ける可能性がある。従って、それらの攻撃から資産を防御し、セキュリティ事件・事故を防止するための策が施される。また、外部ネットワーク(インターネット)と内部ネットワークとの間にファイアウォールで仕切られた安全性の高いセグメント(DMZ: DeMilitarized Zone:非武装地帯)内に設置される。

なお、IPv4 アドレスの枯渇問題を踏まえ、IPv4 と IPv6 の共存や併用が適切に行える様、公開 Web サーバ関連の各種機器に関して、設計時及び機材調達時のみならず、運用・管理・監視・保守等の内容やセキュリティ対策についても、あらかじめ考慮しておくこと。

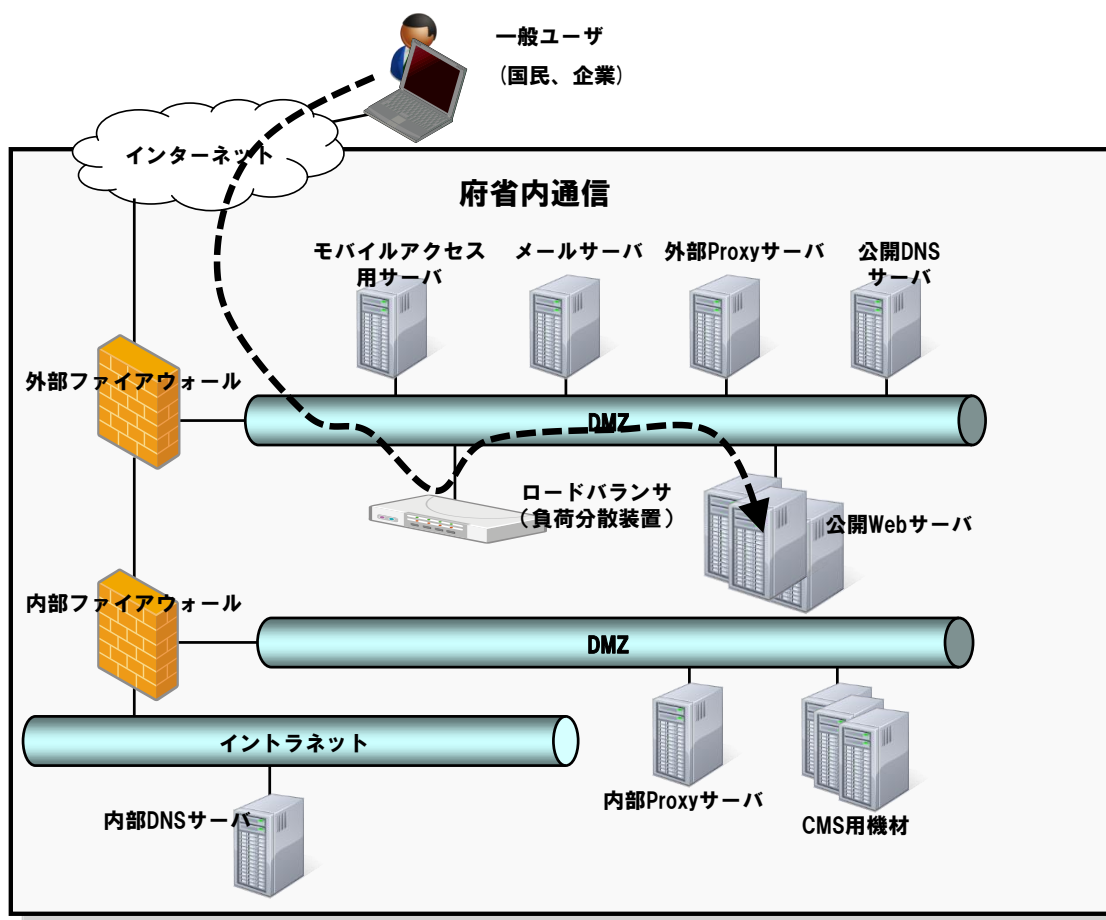



図 5.11-1 公開 Web サーバの配置

公開 Web サーバの機能・サービス	
機能・サービス	定義
WWW サービス	HTTP プロトコルを利用して、主に国民・企業等への情報公開のためのコンテンツ(文書・画像・その他データ)の配信を行うサービス。
FTP サービス	FTP プロトコルを利用して、府省外の端末と公開 Web サーバ間でファイルの送受信(アップロード・ダウンロード)を可能にするサービス。主に大容量又は頻繁に版が更新されるファイル群の配信や、アップロードを行う場合に利用される。
コンテンツ・マネジメント・システム(CMS)	コンテンツ・マネジメント・システム(CMS)とは、公開 Web サーバ上の WWW サービスから公開・配信する Web ベースのデジタルコンテンツ(テキストや画像等)の制作、管理、公開 Web サーバへの配信、維持・保守を行うサービス。内部統制やアクセシビリティへの対応や配慮を行うことを想定した機能を有する。

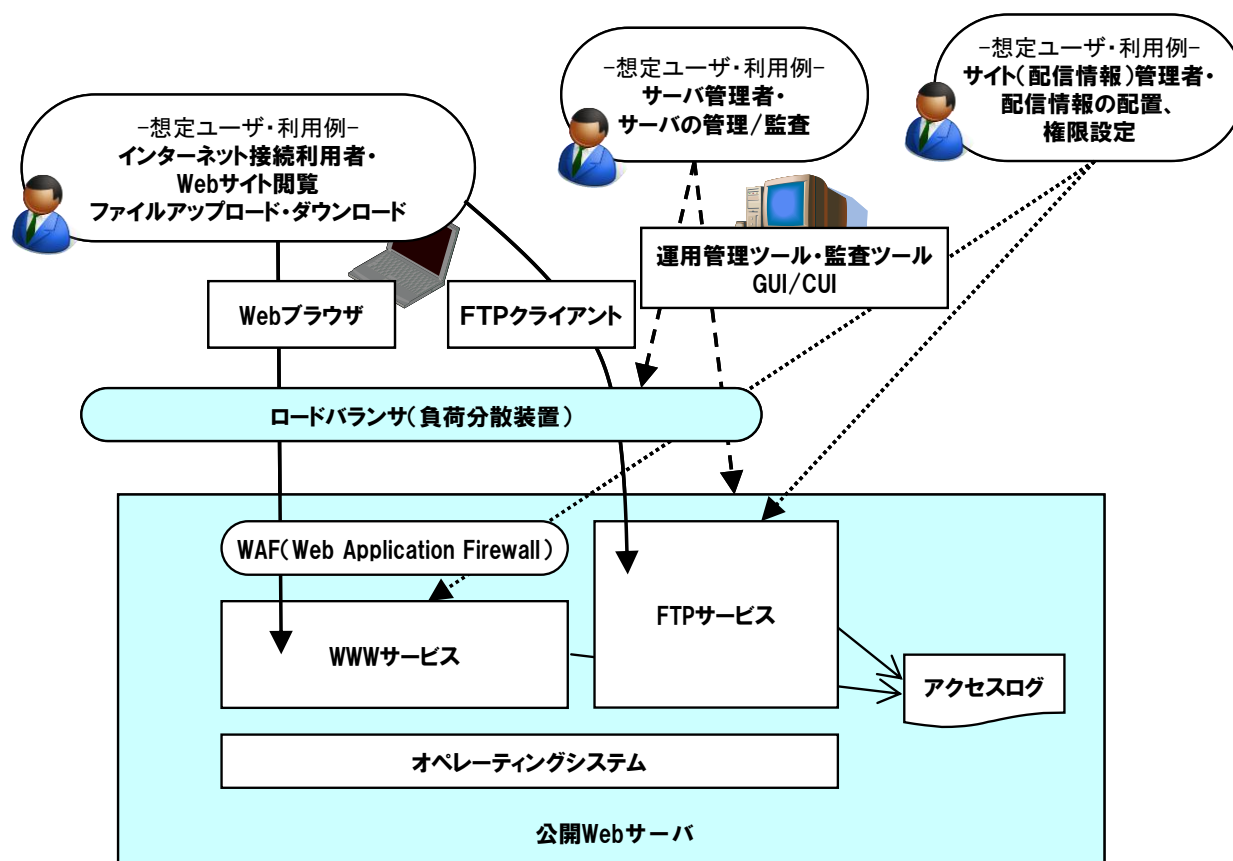



図 5.11-2 公開 Web サーバ概念図

5.11.2.WWW サービス

機能要件		
1	基本	Web ブラウザ等のクライアントからの要求に対して、Web サーバ上に格納されたコンテンツを返送する。加えて、コンテンツに埋め込まれたサーバサイドスクリプト言語【SSI 等】に従いデータ【HTML 等】を変換して送信する機能及びサーバ上で外部プログラムを実行することによって動的にデータを整形(HTML、XML、画像データ等)して送信する機能を有すること。
2	基本	利用者認証・認可：利用者からの公開サイトへのアクセスに対して、個人を特定し、認証(事前に利用を許されている者に対してはサイトの利用・アクセスを許可し、それ以外の者は拒否する)を行う機能を有すること。認証方式は、経路暗号化と基本認証の組み合わせや、ダイジェスト認証等、認証情報の漏えいやなりすましを防げる方式を利用すること。また、利用者ごとに公開 Web サイト内でアクセスできるコンテンツの範囲や操作の権限の設定及び認可を行えること。またこれら認証・認可を外部のディレクトリサービスと連携できること。
3	基本	WAF(Web アプリケーションファイアウォール)：公開 Web サイト上のアプリケーションや Web ページに対する送信情報の内容を検査して、SQL インジェクション や クロスサイトスクリプティング等の攻撃につながる不正なデータを検出し、アクセスを遮断する機能を有すること。
4	加点	サーバ証明書と経路暗号化：サーバ証明書(サーバの公開鍵とサーバの情報)をインストールし、SSL プロトコルで転送データを暗号化できる機能を有すること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
5	基本	配信ファイル形式の管理：Web サイトから配信を許可するファイルの形式(フォーマット)の組み合わせを事前に設定しておき、設定に存在しないファイルの形式は配信できないように構成できること。
6	基本	配信ファイルの配置：Web サイト管理者が、イントラネットや公開 Web サイトから配信するコンテンツの配置及びアクセス権限の設定、コンテンツの更新情報の確認・テストの作業を速やかに実施できること。
7	基本	アクセスログ記録：誰が、何時、何を閲覧したか、最後に情報が閲覧されたのはいつか等の履歴をログファイルとして蓄積できること。ログ情報は、HTTP 通信に関する記録情報のタイプと順序を選択・指定することができ、また W3C 拡張ログファイル形式又は NCSA 共通ログファイル形式で出力できること。
8	加点	監査：アクセスログの中から、監査イベント別、時間別、アクセスユーザ別等の様々な切り口で集計したレポートを出力して、監査の目的で閲覧できること。
9	加点	効率測定：WWW サイトの要求量【同時接続数、平均リクエスト頻度 等】、処理効率【HTTP 処理スループット、レスポンスタイム 等】や資源の消費状況【CPU 利用率 等】を測定する機能を有すること。
10	基本	セッション管理：Web アプリケーションが安全性の高いセッション管理を行うために必要なセッション ID の発行及びセッション情報の維持の機能を提供できること。
11	基本	管理インタフェース：各種管理操作【利用者のアカウントの追加・編集・削除、サイトの権限の設定、配信できるファイルタイプの設定、監査、パフォーマンスモニタリング 等】を内部ネットワーク上の管理者端末から行うための、GUI(Graphical User Interface)又は CUI(Character-based User Interface)ツールの機能を提供すること。また、プログラムから管理タスクを呼び出すための API(Application Program Interface)を提供すること。

非機能要件（個別の要件がある場合のみ記述）		
性能	基本	クライアント(主に Web ブラウザ)からの要求を処理できる十分な処理性能【同時接続数、SPECweb 値　等】を有すること。
可用性	基本	サーバハードウェアやミドルウェアの障害が発生した場合であっても正常な後続の要求処理を継続できる構成【クラスタリング　等】を有すること。
処理能力の拡張性	基本	同時接続数、アクセス量が増加、又は減少した際に、サービスを止めずにサーバの資源の増強/削減、サーバの増設/削減等を行い適切な処理能力を確保できること。
SSL 性能拡張性	基本	SSL プロトコルの暗号化・復号の処理性能を向上させる機構【SSL アクセラレータ　等】を追加できる構成であること。
定期的なミドルウェア・OS へのセキュリティパッチの情報配信	基本	情報セキュリティサービスベンダーの情報提供対象ソフトウェアに含まれ、情報提供サービス等への加入により脆弱性やセキュリティパッチの情報が定期的{月に 1 回程度}にサーバ管理者に配信されること。
ミドルウェア・OS へのセキュリティパッチの適用作業	基本	オペレーティングシステムや Web ページ配信ミドルウェアへのセキュリティパッチの適用、テスト・検証、状況に応じた取り消し(削除)の作業が行えること。
サービス提供時間帯	基本	{24 時間×7 日間/週}の時間帯でサービスを提供できること。
バックアップ・復旧	基本	公開 Web サイト上のデータ(配信コンテンツ及びサーバの構成情報)のバックアップを、Web サイトを停止することなく行え、またそのバックアップデータからサイトの復旧を速やかに行えること。
リモート管理	基本	内部ネットワーク上の管理者端末から公開 Web サイトの管理タスクを実行できる構成を有すること。
負荷分散	基本	公開 Web サーバの前面に配置された負荷分散機能(装置)によって、負荷分散が可能な構成がとれること。

関連する技術	
Web サーバ・クライアント(Web ブラウザ)間通信プロトコル	HTTP(Hyper Text Transfer Protocol)
Web ページ記述言語	HTML(Hyper Text Markup Language) HTML 4.01 仕様(W3C 勧告 1999 年 12 月 24 日)として規格化されている。 CSS(Cascading Style Sheets) CSS2.1 仕様(W3C 勧告 2009 年 9 月 8 日)として規格化されている。
サーバ上で外部プログラムを実行する技術	CGI(Common Gateway Interface) CGI は、RFC3875 として規格化されている。 Java Servlet ASP.NET(Active Server Pages for .NET)
サーバサイドスクリプト言語	SSI(Server Side Include) PHP(Hypertext Preprocessor) JSP(Java Server Pages)
Web 処理効率測定単位	SPECweb
認証方式	基本認証(Basic Authorization) ダイジェスト認証(Digest Authorization)
ディレクトリサービスプロトコル	LDAP(Lightweight Directory Access Protocol)
経路暗号化プロトコル	SSL(Secure Socket Layer)
様々な形式のファイルを電子メール又は HTML プロトコルで送受信するための規格	MIME(Multipurpose Internet Mail Extension)
ログファイル形式	W3C 拡張ログファイル形式 NCSA 共通ログファイル形式
監視・制御機構/プロトコル	SNMP(Simple Network Management Protocol) WBEM(Web-Based Enterprise Management)

5.11.3.FTP サービス

機能要件		
1	基本	クライアント PC と公開 Web サーバの間でのファイル転送を行う際のサーバ側のファイル送受信サービスを提供できること。
2	基本	利用者認証・認可：利用者を特定し、それぞれの権限に合わせて許可される操作や、その対象となるファイルやフォルダへの操作の許可や拒否を行う仕組みを有すること。またこれら認証・認可を OS のアクセス制御機能や外部のディレクトリサービスと連携して行えること。
3	基本	送受信データ暗号化：送受信するファイルのデータや利用者識別子やパスワードを暗号化することができること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
4	基本	ユーザ分離：利用者ごとにアップロード・ダウンロードできる領域（フォルダ）を分離し、ほかの利用者のフォルダから隔離することができること。 利用者用フォルダを指定された構造で作成することができること。また、利用者単位に利用できるフォルダ容量や転送できるファイルの最大サイズを指定できること。
5	基本	アクセスログ記録：誰が、何時、何を、どのような操作を行ったか等の履歴をログファイルとして蓄積できること。ログ情報は、FTP 通信に関する記録情報のタイプと順序を選択・指定することができ、また W3C 拡張ログファイル形式又は NCSA 共通ログファイル形式で出力できること。
6	基本	監査：利用状況ログの中から、監査イベント別、時間別、アクセスユーザ別等の様々な切り口で集計したレポートを出力して、監査の目的で閲覧することができること。
7	基本	クライアントアクセス：クライアント PC から FTP サイトへのアクセスは、Web ブラウザ又は CUI(Character-based User Interface)を利用して行えること。
8	加点	効率測定：FTP サイトの処理要求【同時接続数　等】、処理効率【転送速度　等】やサーバの資源の消費状況【CPU 使用率、I/O キュー待ち数　等】を測定する機能を有すること。
9	基本	管理インタフェース：各種管理操作【利用者のアカウントの追加・編集・削除、サイトの権限の設定、配信できるファイルタイプの設定、監査、パフォーマンスモニタリング　等】を内部ネットワーク上の管理者端末から行うための手段を提供すること。また、管理手段が GUI(Graphical User Interface)又は CUI(Character-based User Interface)ツールである場合は、プログラムから管理タスクを呼び出すための API(Application Program Interface)を提供すること。

非機能要件（個別の要件がある場合のみ記述）		
性能	基本	ファイルのアップロード及びダウンロード処理要求量を処理できる十分な性能【同時接続数、データ転送能力　等】を有すること。
データ許容量	基本	アップロード・ダウンロードするファイルを格納するディスク領域の容量が十分確保されていること。
可用性	基本	単一のサーバのサーバハードウェアや OS、ミドルウェアの障害が発生した場合であっても正常なサーバが後続の要求処理を継続できる構成を有すること。
ディスク領域の拡張性	基本	アップロード・ダウンロードするファイルを格納するディスク領域の空き容量が不足した際に、事前に指定した時間以内に空(あ)き領域の拡張を行えること。
処理能力の拡張性	基本	同時接続数、データ転送要求量が増加、又は減少した際に、サービスを止めずにサーバの資源の増強/削減、サーバの増設/削減等を行い適切な処理能力を確保できること。
定期的なミドルウェア・OS へのセキュリティパッチの情報配信	基本	情報セキュリティサービスベンダーの情報提供対象ソフトウェアに含まれ、情報提供サービス等への加入により脆弱性やセキュリティパッチの情報が定期的{月に 1 回程度}にサーバ管理者に配信されること。
ミドルウェア・OS へのセキュリティパッチの適用作業	基本	オペレーティングシステムや FTP サービスミドルウェアへのセキュリティパッチの適用、テスト・検証、状況に応じた取り消し(削除)の作業が行えること。
サービス提供時間帯	基本	{24 時間×7 日間/週}の時間帯で提供できること。
バックアップ・復旧	基本	FTP サイト上のファイル格納領域のデータのバックアップを、サービスを停止することなく行え、またそのバックアップデータからサイトの復旧を速やかに行えること。
リモート管理	基本	内部ネットワーク上の管理者端末から公開 FTP サイトの管理タスクを実行できる構成を有すること。
負荷分散	加点	複数のサーバを束ねて単一の FTP サイトを構築し、かつデータ通信量の実績が最小のサーバに要求を割り当てることによってファイル転送要求の負荷を分散できる構成を有すること。

関連する技術	
ファイル転送プロトコル	FTP(File Transfer Protocol)
ディレクトリサービスプロトコル	LDAP(Lightweight Directory Access Protocol)
ファイル転送におけるデータ暗号化プロトコル	FTPS (File Transfer Protocol over SSL/TLS) SFTP(Secure File Transfer Protocol)
ログファイル形式	W3C 拡張ログファイル形式 NCSA 共通ログファイル形式
監視・制御機構/プロトコル	SNMP(Simple Network Management Protocol) WBEM(Web-Based Enterprise Management)

5.11.4.コンテンツ・マネジメント・システム(CMS)

機能要件		
1	加点	コンテンツの制作作業において、既存の Web サイトのコンテンツを取り込むことができること。
2	加点	テキスト、画像等のコンテンツ群に対して検索を行い、一覧として閲覧・参照を行いながら効率的にコンテンツの制作を行えること。
3	加点	Web ページのひな形等のテンプレートを活用し、サイト全体で標準化又は統一化したページデザインやアクセシビリティの規格に準拠したコンテンツ作成や統制が容易に行えること。
4	基本	HTML ファイルの編集による更新作業が可能であること。
5	加点	【PDF、Flash、テキスト、Microsoft Office ドキュメント 等】の形式のデータをコンテンツファイルとして扱えること。
6	加点	コンテンツに対する操作の権限を特定の利用者又は利用者グループごとに設定する権限管理及び認証・認可の機能を有すること。また認証・認可の機能はほかのディレクトリサービスと連携することができること。
7	基本	公開予定のコンテンツファイルを登録して、公開後の Web ページのイメージを閲覧できる機能を有すること。
8	加点	公開予定のコンテンツの承認及び公開を自動化又は支援するワークフロー機能を有すること。
9	加点	事前に公開予定のコンテンツファイル及び公開開始日時を指定しておくと、公開開始日時になった時点から、そのコンテンツを自動的に公開 Web サーバから公開の状態にさせる機能を有すること。
10	加点	過去の更新履歴を参照し、また任意の時点の状態でのコンテンツの公開イメージの閲覧や、その時点にコンテンツの内容を戻す等の操作が行えること。
11	加点	コンテンツの制作・保守・運営を行う担当者が実施したファイルへの操作の履歴(誰が、何時、何を行ったのか)を閲覧できること。
12	加点	更新情報配信技術【RSS フィード、ATOM フィード 等】による Web ページ更新情報の配信が可能であること。

非機能要件(個別の要件がある場合のみ記述)		
可用性	加点	CMS が停止しても WWW サービスによるコンテンツの配信が継続できること。
バックアップ・復旧	加点	Web コンテンツのバックアップを制作作業又は配信している最中に実施できること。またバックアップから復元する際には任意の時点のコンテンツに戻せること。

関連する技術	
Web アクセシビリティの確保基準	JIS X 8341-3 W3C WCAG(Web Content Accessibility Guidelines) 1.0/2.0
ディレクトリサービスプロトコル	LDAP(Lightweight Directory Access Protocol)

5.12.グループウェア，ファイルサーバ，メールサーバ

5.12.1.グループウェア，ファイルサーバ，メールサーバの定義

グループウェア，ファイルサーバ，メールサーバは、情報システムの利用者間で情報の交換・共有を実現することで、組織としての生産性を向上させるための仕組みと位置づけられる。電子メール、電子掲示板、電子会議室、スケジュール、会議室予約、ファイル共有等の機能を提供する。これにより、利用者間の円滑なコミュニケーションを実現し、情報共有による政策立案を支援することを目的とする。

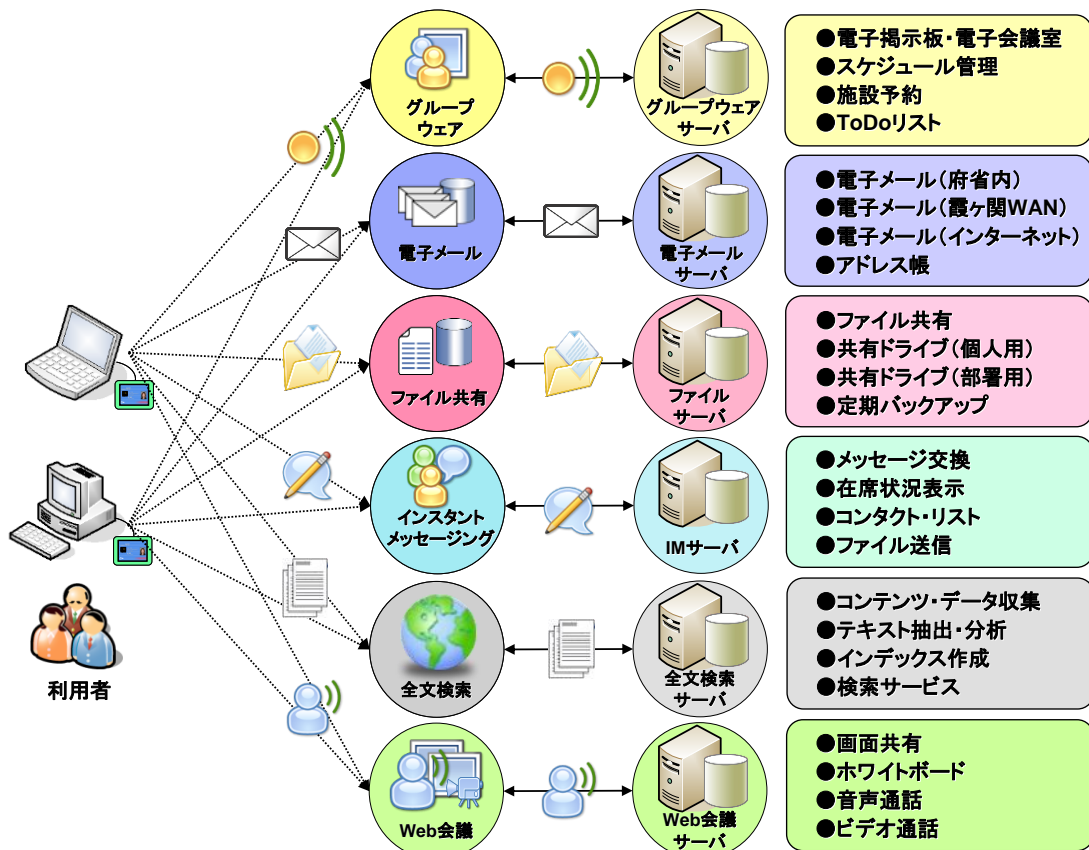



図 5.12-1 グループウェア，ファイルサーバ，メールサーバの機能・サービス

グループウェア，ファイルサーバ，メールサーバの機能・サービスとして、次の 6 つが挙げられる。

① グループウェア
② 電子メール
③ ファイル共有
④ インスタント・メッセージング
⑤ 全文検索
⑥ Web 会議

グループウェア，ファイルサーバ，メールサーバの機能・サービス	
機能・サービス	定義
グループウェア	利用者間で情報共有を行い、円滑なコミュニケーションを実現するための機能を提供する。利用者は、電子掲示板や電子会議室の機能により、意見交換や情報交換を行うことができる。利用者のスケジュール管理や会議室等の設備管理、ToDo リスト等の機能により、日々の職務遂行の生産性向上に寄与する。利用者に割り当てるユーザ ID や利用者が所属するグループ等の属性情報を管理する機能も提供し、職員ディレクトリとしての利用も可能である。
電子メール	利用者が省庁内、省庁外との電子メールの送受信を行う機能を提供する。標準的なメール送受信のプロトコルを採用し、端末からの送信要求は SMTP、受信要求は POP、IMAP に対応する。機密性の高い内容の電子メールを交換することを想定し、電子メールの暗号化や電子署名にも対応する。電子メールによるウイルス感染を防止するために、添付ファイルのウイルス・チェックも行うこととする。なお、電子メールは、グループウェアの機能として提供されるケースもある。
ファイル共有	利用者間での情報共有を容易かつ迅速に行うために、端末間でストレージを共有して、ファイル共有を実現する機能である。ファイルサーバで管理するストレージ領域を利用者間で共有し、利用者の所属や権限に応じたファイル共有を実現する。ファイルの共有に際しては、厳密なアクセス制御を実装し、アクセス履歴は監査ログとして取得する。
インスタント・メッセージング	利用者の使用状況を確認して、リアルタイムでメッセージを交換できる機能を提供する。利用者の使用状況は、オンライン/オフラインだけでなく、オンライン時には、応答可能/応答不可/離席中/会議中等で確認できるため、相手の都合により、適切な連絡手段(電話や電子メール、インスタント・メッセージング等)を選択することができる。
全文検索	グループウェアが提供する文書データベースやファイルサーバ上に蓄積された多くの文書ファイルから、指定された文字列を検索する機能を提供する。検索においては、単一又は複数のキーワードと、キーワード間の条件(AND、OR 等)を指定できる。検索結果は、利用者のアクセス権限に応じて、権限内の情報だけが表示される。
Web 会議	ネットワーク上の複数の利用者が、画面を共有しながら音声通話やビデオ会議を行うことにより、会議を開催できる。オフィス文書の共有機能や、会議の参加者が文字や図を書き込みできる仮想的なホワイトボード機能も提供する。Web 会議の予約や管理を行うための Web インタフェースが提供される。

5.12.2.グループウェアの機能要件・非機能要件・標準技術

機能要件		
1	基本	利用者が電子掲示板に対して掲示文書の登録/変更/削除が行えること。
2	基本	掲示文書に対して、ファイルや表、画像、文書等へのリンクを添付できること。
3	基本	掲示文書の一覧画面より、作成者別やカテゴリ別等の条件で掲示文書を分類できること。また、【キーワード　等】の条件で掲示文書を検索できること。
4	基本	システム管理者は、必要に応じて各電子掲示板にアクセス可能な利用者を定義し、使用制限を設定できること。
5	基本	掲示不適切な内容が電子掲示板に掲載された場合には、システム管理者が文書を削除することができること。
6	基本	電子会議室の機能を提供し、複数の利用者が特定のテーマについて意見交換(書き込み)を行うことができること。
7	基本	利用者の意見(書き込み)は、電子データとして保存され記録されることとし、議論を行うテーマごとに電子会議室を作成できること。
8	加点	特定の話題(テーマ)に関する一連の書き込みは、階層的に表示を行い、スレッドとしてわかりやすく表示できること。
9	基本	利用者単位でスケジュール管理ができること。スケジュールを他の利用者に公開できることとし、スケジュールを公開する利用者の範囲を設定、管理できること。
10	基本	同じ組織/グループに所属する複数の利用者の予定閲覧や空き時間の検索ができること。
11	基本	毎週や毎月等の繰り返しスケジュールの登録や、スケジュール登録依頼の受容と拒否ができること。
12	加点	スケジュールが重なっている場合には、目印等の表示で認識可能であること。
13	基本	利用者が設備(会議室等)の予約及び予約状況の参照を行えること。
14	基本	管理者が設備の登録、更新、削除の管理を行えること。設備ごとにアクセス権の設定が可能であること。
15	基本	利用者が予約を行う際に、指定した会議室の空き時間を検索できること。また、指定した時間帯に利用可能な会議室を検索できること。
16	基本	電子メール等と連動して、会議室を予約した際に、関係者へ通知を送信できること。
17	基本	利用者が作成した ToDo リストを管理できること。
18	基本	ToDo リストに登録されるタスク(作業)には、開始日や終了期限、優先度等の項目を指定でき、作業の進捗(しんちょく)状況を管理できること。
19	基本	利用者を一元的に管理するディレクトリとともに、電子電話帳の機能を提供すること。【名前、所属、電話番号、メールアドレス　等】で利用者の検索ができること。
20	基本	グループウェアを利用する際には、利用者ごとに割り当てられたユーザ ID とパスワードにより認証を行うこと。
21	基本	グラフィカルな利用者インタフェース(GUI)を用意し、利用者が容易に利用できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	グループウェアで提供する電子【掲示板、電子会議室、スケジュール、施設予約、ToDo リスト、電子電話帳　等】の各機能においては、厳密なアクセス制御が行えること。
	加点	通信を暗号化し、セキュリティを確保できること。
パフォーマンス	基本	｛約 5 万｝の利用者を想定してシステムの設計を行うこと。事前に明示された性能要件に対して、十分な処理能力をもった構成とすること。
拡張性	加点	対象とする利用者の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	設定情報とともに、利用者が作成したコンテンツ(【書き込み、スケジュール、予約、タスク　等】)のバックアップを取得できること。

関連する技術	
ディレクトリ・サービス・プロトコル	LDAP(Lightweight Directory Access Protocol)は、ディレクトリ・サービスに接続するために使用される標準プロトコル。LDAP V3 が規定されている。
ディレクトリ交換フォーマット	LDIF(LDAP データ交換フォーマット：LDAP Data Interchange Format)は、LDAP のアカウント情報を交換する際に用いるファイル・フォーマットである。

補足：広義のグループウェアの定義では、電子メールやインスタント・メッセージング、Web 会議等の機能を含むケースもある。調達の範囲に応じて適切な仕様記述を採用すること。

5.12.3.電子メールの機能要件・非機能要件・標準技術

機能要件		
1	基本	Web メール及び電子メール・クライアントからメールの作成及び送受信ができること。電子メール・クライアントからの送信要求は SMTP、受信要求は POP、IMAP に対応すること。また、Web メールは HTTP/HTTPS に対応すること。
2	基本	メール形式は、テキスト形式のメールのほか、HTML 形式のメールにも対応すること。
3	基本	メールは、宛先(あてさき)や内容により分類して整理できること。メールを整理するフォルダは階層的に作成でき、条件を指定して参照したいメールを検索できること。
4	基本	フォルダに対して、送信者、主題中のキーワードをもとにメールの自動振り分けを行う機能を有すること。メールを振り分けるアドレスやキーワードは、利用者が複数指定できること。
5	基本	日本語の名前や組織名に対応したアドレス帳の機能を提供すること。
6	基本	機密性の高い内容の電子メールを交換する場合は、メールの本文及び添付ファイルの暗号化ができること。送信者認証及び電子署名の付与と確認が行えること。暗号化と電子署名は S/MIME に対応していること。
7	加点	利用者の不在に合わせて、メール送信元に不在である旨を通知できること。
8	基本	電子メール・クライアントでは、ネットワークがオフラインの状態でもメールの参照や作成が行えること。
9	加点	電子メール・クライアントではメールが誤って転送されたり、コピー＆ペーストや印刷で転用されたりすることを防止するための仕組みを有すること。
10	基本	利用者が使用できるメールボックスのサイズに制限をかけることができること。
11	基本	スケジュール登録時に自動的に参加者にメールが送付される等、グループウェアのスケジュール管理や施設予約の機能と連携ができること。
12	加点	メールの開封確認の設定が行えること。
13	加点	メールに添付されたファイルは、ウイルス対策ソフトによりメールサーバ上でチェックできること。ただし、暗号化されたメールについてはメールサーバ上でのウイルス・チェックが困難であるため、別途端末上等でウイルス・チェックを行えること。
14	加点	メールの不正利用や情報漏えいを防止するために、監査目的でメールのアーカイブを保存できること。
15	加点	府省内のメールサーバの IP アドレス等の物理的な情報がメールのヘッダに付随して府省外に漏えいしないよう設定すること。
16	加点	電子メール・クライアントからの送信要求は認証を行い SMTP over SSL/TLS に対応、受信要求は POP over SSL/TLS、IMAP over SSL/TLS に対応すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	加点	電子メールの改ざん、なりすましを防ぐために、送信ドメイン認証による電子メール検証を行って、不正なメールを検出することができること。
	加点	メールの誤送信を防ぐため、メールの配信を一定期間待機させ、その間に宛先(あてさき)相違に気がついた場合には、送信を中止できる等の誤送信防止機能を有すること。
	加点	機密性が高いケースでは、承認者がメール内容を確認後、承認を行ったメールのみを送信する仕組みを有すること。
パフォーマンス	基本	{約 5 万}の利用者を想定してシステムの設計を行うこと。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
	加点	メールボックスのサイズは、1 利用者あたり{100MB}を確保すること。
拡張性	加点	対象とする利用者の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	設定情報とともに、利用者が送受信したメールのバックアップを取得できること。

関連する技術	
メール送信プロトコル	SMTP(Simple Mail Transfer Protocol)は、電子メールを送信する際に使用する標準プロトコル。利用者が電子メールをメールサーバに送信する際や、メールサーバ間で電子メールが転送される際に利用される。
メール受信プロトコル	POP3(Post Office Protocol)は、電子メールを保存しているメールサーバからメールを受信するためのプロトコル。利用者が電子メールをメールサーバから受信する際に利用される。メールの保存・管理は端末上で行う。
	IMAP4(Internet Message Access Protocol)は、電子メールを保存しているメールサーバからメールを受信するためのプロトコル。利用者が電子メールをメールサーバから受信する際に利用される。メールサーバ上でメールを保存・管理できる。
メール暗号化方式	S/MIME(Secure/Multipurpose Internet Mail Extensions)は、電子メールの暗号化と電子署名を行うための標準方式。利用者が電子メールを暗号化したり、電子署名を行う際に利用される。

補足：電子メールの利用については、府省内でのメール交換と、府省外やインターネットとのメール交換では、調達すべき仕組みが異なるケース(メール・ゲートウェイの設置等)が想定される。調達にあたっては、府省内/府省外/インターネットのうち、メール交換の範囲をどこまでとするかを明示する必要がある。

(例)

【本調達では、本省内部でのメール交換のみを対象とする。】

【本調達では、本省内部だけでなく、霞が関 WAN や LGWAN を経由して、他省庁や地方公共団体とのメール交換を対象とする。】

【本調達では、本省内部と他省庁に加え、インターネット経由で民間とのメール交換を対象とする。】

5.12.4.ファイル共有の機能要件・非機能要件・標準技術

機能要件		
1	基本	利用者間で、ファイルの共有を行う機能を提供すること。
2	基本	OS 標準のファイル管理ソフトウェア又は Web ブラウザから共有リソースへアクセスできること。
3	基本	利用者の権限に応じてアクセス権を設定し、アクセス制御ができること。アクセス制御は、ファイル又はフォルダ単位に作成、参照、更新、削除を管理できること。
4	基本	共有リソースへのアクセス・ログを記録し、不正アクセス等の分析を行うための情報を出力できること。
5	基本	ファイルサーバ上に格納するデータは暗号化できること。
6	基本	利用者が誤ってデータを削除してしまった場合に容易に復元を行うために、バックアップを定期的に取得できること。
7	基本	ディスクの利用容量管理のために、利用者もしくは、共有ドライブごとに、使用できるディスク容量に制限をかけることができること。
8	加点	ファイルサーバ上のファイルは全文検索機能の検索対象となること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
	加点	ストレージに関しても RAID 技術によりディスク障害に備えること。
セキュリティ	基本	ファイルサーバに格納するデータに対して、不正アクセスによる情報漏えいや改ざんを防止する仕組みを有すること。
	加点	通信を暗号化し、セキュリティを確保できること。
パフォーマンス	基本	{約 5 万}の利用者を想定してシステムの設計を行うこと。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
	加点	同時に{300 端末}からのアクセスに対応できること。
	加点	ファイルサーバの容量は、実効容量{100TB}以上とすること。
拡張性	加点	対象とする利用者の増加が予想されるため、処理能力やディスク容量の柔軟な増強ができる構成とすること。
バックアップ	基本	設定情報とともに、共有ディスク上のデータのバックアップを取得できること。

関連する技術	
ファイル共有プロトコル	CIFS(Common Internet File System)は、TCP/IP のネットワーク上でファイル共有を行うための標準プロトコル。

5.12.5.インスタント・メッセージングの機能要件・非機能要件・標準技術

機能要件		
1	基本	端末上で利用者の使用状況を確認して、リアルタイムでメッセージを交換できる仕組みを提供すること。
2	基本	メッセージ交換を行う相手は、利用者固有のコンタクト・リストとして、利用者をグループ分けして管理できること。
3	基本	コンタクト・リスト上の利用者については、オンラインかオフラインかの識別ができるように、在席状況を表示すること。
4	基本	オンライン時に表示する利用状況は、”応答可能”、”応答不可”、”離席中”、”会議中”等から利用者自身が選択できること。
5	基本	利用者の在席状況を公開するとともに、電話番号やメールアドレス等の利用者の属性情報を表示できること。
6	基本	メッセージ交換内容の履歴を相手の利用者ごとに保存することができること。
7	基本	1 対 1 のメッセージ交換だけでなく、3 人以上の利用者でもメッセージ交換ができること。
8	基本	オンラインの状態において、一定時間、利用者が端末を操作しない場合は、自動的に”離席中”に利用状況を変更することができること。
9	基本	ファイル送信機能を提供すること。メールへの添付等を介さずに、メッセージ交換と同じ仕組みでファイル交換を行うことができること。
10	基本	インスタント・メッセージングを利用する際には、利用者ごとに割り当てられたユーザ ID とパスワードにより認証を行うこと。
11	基本	グラフィカルな利用者インタフェース(GUI)を用意し、利用者が容易に利用できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	加点	通信を暗号化し、セキュリティを確保できること。
パフォーマンス	基本	{約 5 万}の利用者を想定してシステムの設計を行うこと。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とする利用者の増加が予想されるため、処理能力やディスク容量の柔軟な増強ができる構成とすること。
バックアップ	基本	設定情報とともに、コンタクト・リスト等のデータのバックアップを取得できること。

5.12.6.全文検索の機能要件・非機能要件・標準技術

機能要件		
1	基本	利用者が入力したキーワードを含む府省内のコンテンツを検索できること。検索においては、単一又は複数のキーワードとキーワード間の条件(AND、OR 等)を指定できること。
2	基本	検索範囲は、利用者がアクセス権限をもつ府省内のコンテンツに限定すること。
3	基本	検索対象は、ファイルサーバ上に格納されたワードプロセッサ、表計算、プレゼンテーション等のオフィス・アプリケーションにより作成した文書、グループウェア上の電子掲示板等の文書データベース、Web サイト上の XML 及び HTML ファイルの内容等とする。
4	基本	ファイルサーバ上に保存されたデータのみのように、検索対象の選択、絞り込みができること。
5	基本	入力したキーワードに対して、類義語検索ができること。類義語検索のためのデータをもち、この辞書を管理者がメンテナンスできること。
6	基本	検索結果の情報の一覧表示を行うことができ、利用者が一覧表示内の情報を選択した際には、当該情報を表示及び保存できること。
7	加点	定期的に府省内に設置されたファイルサーバやグループウェア、Web サイトへアクセスして、検索対象となるデータを収集すること。
8	加点	収集したテキスト/HTML/XML ファイルやオフィス・アプリケーションで作成した文書から、テキストを抽出し分析を行うこと。
9	加点	分析結果をもとにして、検索の高速化のために、検索対象のインデックスを作成すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	検索範囲は、利用者がアクセス権限をもつコンテンツに限定すること。
	加点	通信を暗号化し、セキュリティを確保できること。
	加点	SQL インジェクション等、利用者からのセキュリティ的な攻撃に対する耐性をもつこと。
パフォーマンス	基本	{約 5 万}利用者を想定してシステムの設計を行うこと。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とする利用者の増加が予想されるため、処理能力やディスク容量の柔軟な増強ができる構成とすること。
バックアップ	基本	設定情報とともに、インデックス等のデータのバックアップを取得できること。

5.12.7.Web 会議の機能要件・非機能要件・標準技術

機能要件		
1	基本	ネットワーク上の複数の参加者が、ブラウザの共有画面を利用した Web 会議を行えること。
2	加点	端末で利用可能なマイクとスピーカー、Web カメラを利用して、音声通話やビデオ会議が可能なこと。
3	基本	Web 会議に参加している利用者のリストを画面上で確認できること。
4	基本	発表者として指定された参加者の端末画面を、参加者の間で共有できること。
5	基本	画面共有は、発表者の都合に合わせ、画面全体の共有を行うケース、指定アプリケーションの画面のみ共有するケースから選択できること
6	基本	参加者が自由に文字や図を書き込める仮想的なホワイトボードを、参加者の間で共有し議論が行えること。
7	基本	ブラウザから Web 会議の予約を行い、議長となる利用者へメールで通知する仕組みを提供すること。
8	基本	Web 会議の予約の際には、会議名称、日時、参加人数とともに、参加するために必要となるパスワードを指定できること。
9	基本	繰り返し開催される Web 会議の予約を一括して行うために、“毎日”、“毎週”、“毎月”、“毎年”の単位で複数の Web 会議を予約できること。
10	基本	進行中の Web 会議、完了した Web 会議、予約済みの Web 会議のリストが参照できること。
11	基本	利用者自身が議長として開催する Web 会議のリストと詳細情報を参照できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	Web 会議ごとにパスワードを設定でき、あらかじめパスワードを通知された利用者だけが利用できること。
	加点	通信を暗号化し、セキュリティを確保できること。
パフォーマンス	基本	{約 5 万}の利用者を想定してシステムの設計を行うこと。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
	加点	Web 会議への同時参加利用者数は、{約 500 人}とする。
拡張性	加点	対象とする利用者の増加が予想されるため、処理能力やディスク容量の柔軟な増強ができる構成とすること。
バックアップ	基本	Web 会議に関する設定情報等のデータのバックアップを取得できること。

関連する技術	
分散ファイルシステムプロトコル	WebDAV(Web-based Distributed Authoring and Versioning) – HTTP を拡張した Web ベースの分散ファイルシステム向けのファイル管理プロトコル。IETF RFC 2518。

5.13.統合アカウント管理・認証・認可(アクセス制御)

5.13.1. 統合アカウント管理・認証・認可(アクセス制御)の定義

統合アカウント管理・認証・認可(アクセス制御)は、情報システムの利用者を統合的、一元的に管理する仕組みを提供する。利用者がその ID をもっている本人であることを確認し、利用者の権限に基づきリソースへのアクセス制御を行う。

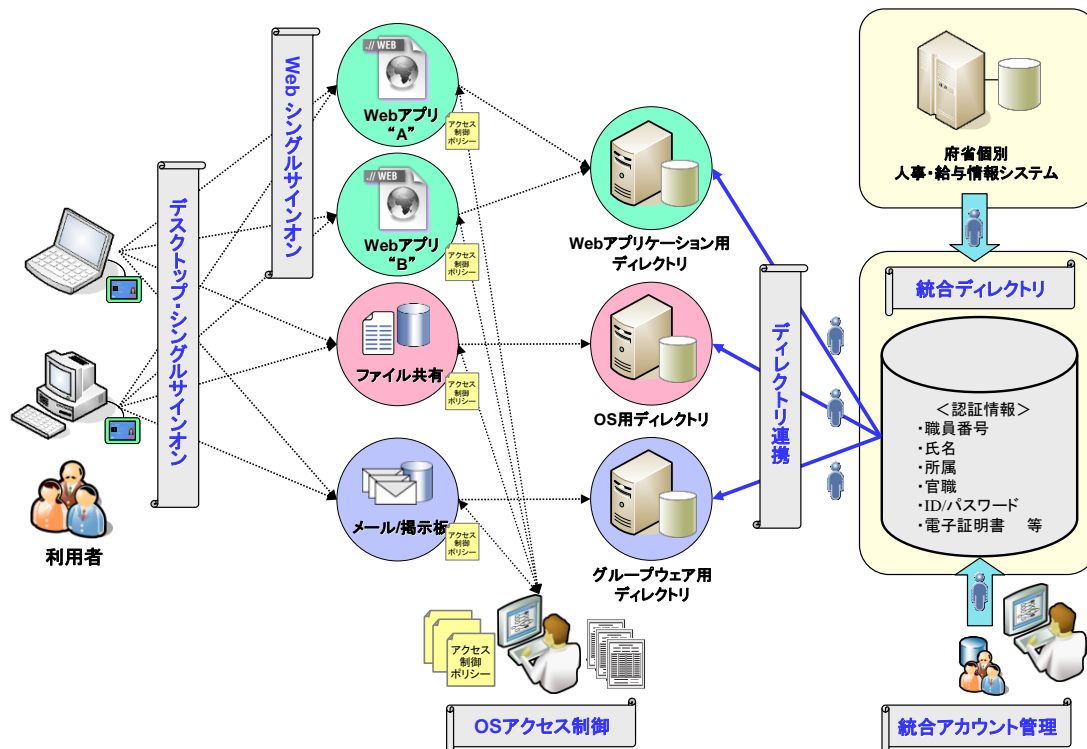



図 5.13-1 統合アカウント管理・認証・認可(アクセス制御)の機能・サービス

統合アカウント管理・認証・認可(アクセス制御)の機能・サービスとして、次の5つが挙げられる。

①統合アカウント管理
②ディレクトリ連携
③Web シングルサインオン
④デスクトップ・シングルサインオン
⑤OS アクセス制御

これらの機能・サービスにより、アカウント情報を一元的に管理する仕組みと、利用者の利便性向上に寄与するシングルサインオン環境が実現される。統合ディレクトリの情報は、組織内の電子電話帳、メールシステム

の共有アドレス帳、インスタント・メッセージングの宛先に活用することも考えられる。

統合アカウント管理・認証・認可(アクセス制御)の機能・サービス	
機能・サービス	定義
統合アカウント管理	利用者の認証情報(ユーザ ID、パスワード)と属性情報(グループ、所属部門等)を一元的に管理する機能を提供する。一元的に管理されたアカウント情報は、あらかじめ定義されたポリシーに基づいて、関連するシステムやディレクトリへ自動又は手動で反映される(プロビジョニング機能)。アカウント管理に関する各種管理業務を支援するためのワークフロー機能も提供する。
ディレクトリ連携	アカウント情報が、RDB や LDAP、CSV ファイル等異なる方式のディレクトリに格納されている環境において、各種ディレクトリやデータベースへ接続するコネクタ機能とアカウント情報の属性を変換(データ変換/マッピング)する機能により、ディレクトリ間の連携を実現する。
Web シングルサインオン	複数の Web アプリケーションに対する認証とアクセス制御を一元的に管理し、シングルサインオンを実現する。利用者は、Web シングルサインオンへ 1 度だけログインすれば、アクセスが可能なすべての Web アプリケーションを個別にログインすることなく利用することができる。Web アプリケーションへのアクセス履歴の記録や、タイムアウトにより再認証を要求する機能も提供する。
デスクトップ・シングルサインオン	端末の OS だけでなく、グループウェアや Web アプリケーション、C/S 型アプリケーション等に一括してログインし、シングルサインオンを実現する。利用者は、デスクトップ・シングルサインオンへ 1 度だけログインすれば、端末上の利用可能なアプリケーションを個別にログインすることなく利用することができる。
OS アクセス制御	あらかじめ定義したアクセス制御ポリシーに従って、OS のリソース(ファイルやネットワーク、ユーザ等)に対するアクセス制御を行う。アクセス制御ポリシーは集中的に管理され、管理対象のシステムに対して一括で適用することができる。いつ、誰が、どのリソースへアクセスし、成功したか/失敗したかといった情報を監査ログとして取得し、蓄積する機能も有する。アクセス制御ポリシーは、一般のユーザだけでなく、いわゆる管理者ユーザと呼ばれる特権ユーザに対しても、管理者の作業内容に合わせて適用することができる。

5.13.2. 統合アカウント管理の機能要件・非機能要件・標準技術

機能要件		
1	基本	アカウント情報の登録/変更/削除を一元的に行う機能を提供すること。
2	基本	アカウント情報の登録/変更/削除等、ポリシーを作成しておくことで、アカウント情報のライフサイクル管理を自動化できること。
3	基本	定義されたポリシーに基づいて、利用者の登録や属性変更を、自動的に宛先(あてさき)のシステムに反映するための仕組み(プロビジョニング機能)を提供すること。
4	基本	ユーザ ID について、命名規則や有効期限等の制約事項に基づき制限をかけることができること。パスワードについても長さや文字種、有効期限等を制限することができること。
5	基本	アカウント情報の登録/変更/削除等の申請後、ワークフローによる承認を経て、各種 OS やディレクトリへ適用する仕組みを有すること。
6	基本	ユーザ ID に対して利用停止(非アクティブ化)と利用再開(アクティブ化)の設定ができること。
7	基本	利用者は、自分自身でパスワードの変更作業やリセット作業が可能なこと(セルフケア)。
8	基本	アカウント情報やポリシーの追加・変更・削除等、重要な操作を監査ログに記録すること。
9	加点	監査ログはレポートとしてわかりやすい形式で表示できること。

非機能要件(個別の要件がある場合のみ記述)		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	認証を受けた管理者のみが、アカウント情報にアクセスできる仕組みを有すること。
	基本	管理者の役割や管理対象の範囲に応じて、適切なアクセス権を設定してアカウント情報を保護することができること。
	基本	長期間使われていないユーザ ID を識別して、無効又は削除できること。
	加点	通信の暗号化が可能なこと。
パフォーマンス	基本	{約 5 万}のアカウントを管理することとなり、人事異動の際には短期間に大量のユーザ属性を更新することが求められる。事前に明示された性能要件に対して、十分な処理能力をもった構成とすること。
拡張性	加点	対象とするシステムや利用者の増加に伴い、アカウントの増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	アカウント情報やポリシーのバックアップを取得ができること。

関連する技術	
ディレクトリサービスアクセスプロトコル	LDAP(Lightweight Directory Access Protocol) – ディレクトリ・サービスに接続するために使用される標準プロトコル。LDAP V3 が規定されている。
ディレクトリサービス交換形式	LDIF(LDAP Data Interchange Format) – LDAP のアカウント情報を交換する際に用いるファイル・フォーマットである。
プロビジョニング情報交換言語	SPML(Service Provisioning Markup Language) – ID プロビジョニングのための標準プロトコル。SPML V2 が規定されている。

・政府機関統一基準に対応する項目:2.1.1.1～2.1.1.4

・物理構成モデルのセグメントに対応する項目:S1～S6

5.13.3. ディレクトリ連携の機能要件・非機能要件・標準技術

機能要件		
1	基本	複数のディレクトリを連携し、格納されているアカウント情報の内容を同期させる機能を提供すること。
2	基本	コネクタ(データ通信)機能を提供すること。分散された各種ディレクトリ【RDB、LDAP、CSV ファイル 等】に対して、アカウント情報を配信することができること。
3	基本	マッチング・エンジン(データ変換/マッピング)機能を提供すること。アカウント情報を配信する際に、宛先(あてさき)ディレクトリの環境に合わせて、データの型変換、マッピングを行うことができること。
4	基本	データ変換やマッピングの設定を行うためのツール【GUI、SDK 等】を提供すること。
5	基本	複数のディレクトリから取得したデータを結合したり加工したりする等、運用中にロジックを自由に組み込むことができること。
6	基本	統合ディレクトリに格納されたパスワードを同期するための仕組みを提供すること。
7	基本	ディレクトリに格納されたアカウント情報に矛盾がないか、不正なアカウントが追加されていないかの棚卸しを行う仕組みを提供すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	加点	通信の暗号化が可能なこと。
パフォーマンス	基本	{約 5 万}のアカウントを管理することとなり、人事異動の際には短期間に大量のユーザ属性を更新することが求められる。事前に明示された性能要件に対して、十分な処理能力をもった構成とすること。
拡張性	加点	対象とするシステムや利用者の増加に伴い、アカウントの増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	マッチング・ルール等の管理データのバックアップを取得すること。

関連する技術	
ディレクトリサービスアクセスプロトコル	LDAP(Lightweight Directory Access Protocol) － ディレクトリ・サービスに接続するために使用される標準プロトコル。LDAP V3 が規定されている。
データベース接続 API	JDBC(Java Database Connectivity) － Java プログラムから RDB へアクセスするための API。ディレクトリが RDB のケースでは利用が想定される。

・政府機関統一基準に対応する項目：2.1.1.1～2.1.1.4

・物理構成モデルのセグメントに対応する項目：S1～S6

5.13.4. Web シングルサインオンの機能要件・非機能要件・標準技術

機能要件		
1	基本	Web アプリケーションに対して、指定された認証方式【ユーザ ID、パスワード 等】による認証と、URL をベースとしたアクセス制御の機能を提供すること。
2	基本	利用者は一度だけログインを行えば、アクセスが可能なすべての Web アプリケーションを個別にログインすることなく利用することができること(シングルサインオン)。
3	基本	アクセス制御ポリシーを集中管理して、複数の認証プロキシやエージェントへ同時に適用できること。
4	基本	ログインした利用者のアカウント情報【ユーザ ID、所属 等】を、Web アプリケーションに対して渡す仕組みを有すること。
5	基本	あらかじめ決められた回数、ログインに失敗したアカウントを、自動的にロックして使用不能にできること。
6	基本	アカウントの認証履歴を、監査ログとして取得し、蓄積できること。
7	加点	トークン認証(ワンタイム・パスワード)、IC カード認証、生体認証等の強力な認証方式と組み合わせることが可能であること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	取得した監査ログはアクセス制御を徹底して改ざんを防止すること。
	加点	通信の暗号化が可能なこと。
パフォーマンス	基本	{約 5 万}のアカウントが想定される。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とする Web アプリケーションや利用者の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	アクセス制御ポリシー等の設定情報や監査ログはバックアップを取得すること。

関連する技術	
ディレクトリサービスアクセスプロトコル	LDAP(Lightweight Directory Access Protocol) – ディレクトリ・サービスに接続するために使用される標準プロトコル。LDAP V3 が規定されている。

・政府機関統一基準に対応する項目：2.1.1.1～2.1.1.4

・物理構成モデルのセグメントに対応する項目：S1～S6

5.13.5. デスクトップ・シングルサインオンの機能要件・非機能要件・標準技術

機能要件		
1	基本	端末上で稼動するエージェントが、利用者に代わってユーザ認証を行うことにより、Web アプリケーションやグループウェア、C/S 型アプリケーション等に自動的にログインし、シングルサインオンを実現すること。
2	基本	利用者はデスクトップに一度ログオンすれば、端末上の利用可能なアプリケーションをログインの手間をかけずに利用することができること。デスクトップ OS のログオン認証と連携するアプリケーションの採用、又は、あらかじめユーザ ID とパスワードを登録して利用するアプリケーションに合わせてエージェントが認証情報を自動的に入力することにより、シングルサインオンを実現する。
3	基本	シングルサインオンの対象とするアプリケーションや自動入力されるユーザ ID とパスワードは、システム管理者が一元的に管理できること。端末の設定を集中管理できること。
4	加点	デスクトップ・シングルサインオンのエージェントへログインする際のパスワードを利用者が忘れた場合を考慮し、パスワードリマインダ機能等のパスワード忘れ時の対応機能があること。
5	加点	トークン認証(ワンタイム・パスワード)、IC カード認証、生体認証等の強力な認証方式と組み合わせることが可能であること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	自動入力されるユーザ ID とパスワードは、暗号化して保持すること。
パフォーマンス	基本	{約 5 万}のアカウントが想定される。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とするアプリケーションや利用者の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	エージェントの設定情報はバックアップを取得すること。

・政府機関統一基準に対応する項目：2.1.1.1～2.1.1.4
・物理構成モデルのセグメントに対応する項目：S1～S6

5.13.6. OS アクセス制御の機能要件・非機能要件・標準技術

ここでは OS に限定したアクセス制御の機能要件、非機能要件のみを記載している。しかし、最近のインターネット技術の発達により、アイデンティティ管理の一環として OS に限定しないアクセス制御技術や権限管理の仕組みが標準化(RBAC や XACML 等)されている。OS に限定しない方式は、あらかじめ定義したアクセス制御ポリシーに従い、リソースに対するアクセス制御情報を配布する。アクセス制御ポリシーは集中的に管理され、作成、変更、削除の監査、ライフサイクル管理機能を有する。アクセス制御はロールベース、ルールベースでの定義が可能で、独自のロジックの組み込みが可能となる。

機能要件		
1	基本	OS のリソース(ファイルやネットワーク、ユーザ等)に対するアクセスを監視して、あらかじめ定義されたアクセス制御ポリシーで許可されたアクセスのみを許可すること。
2	基本	OS の管理者権限をもつアカウントに対してもシステム操作やファイル、プログラムへのアクセスを制御すること。
3	基本	アクセス制御ポリシーを集中管理して、複数の管理対象サーバへ適用できること。
4	基本	重要データ、プログラムの改ざん防止及び検知ができること。
5	基本	不正アクセス等のポリシー違反を検知した場合は、監視コンソールへ通知できること。
6	加点	OS のリソース(ファイルやネットワーク、ユーザ等)に対するアクセスの監査ログとして【日時、ユーザ名、リソース名、アクセス内容、アクセス結果　等】の内容を記録すること。
7	加点	不正アクセス等のポリシー違反を検知した場合は、記録された監査ログを参照することにより、【不正アクセスの日時、ユーザ名、リソース名、アクセス内容、アクセス結果　等】の情報を分析することができること。
8	基本	管理対象サーバ上で取得された監査ログを収集し、一元的に管理・保管する仕組みを有すること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	取得した監査ログはアクセス制御を徹底して改ざんを防止すること。
	加点	通信の暗号化が可能なこと。
パフォーマンス	基本	{約 5 万}のアカウントが想定される。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とするシステムや利用者の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	アクセス制御ポリシー等の設定情報や監査ログはバックアップを取得すること。

関連する技術	
アクセス制御	RBAC (Role Based Access Control) － ロールをもとにアクセス制御を実行する考え方。管理者はユーザ(あるいはグループ)とロールの紐(ひも)付け(User Role Assignment: UA)とロールと権限の紐(ひも)付け(Permission Role Assignment: PA)を管理することで適切な権限の付与を実現する。
アクセスコントロール記述言語	XACML(eXtensible Access Control Markup Language) － XML ベースのアクセス制御ポリシーを記述するための言語仕様。リソースに対し複雑な条件を設定することが可能となっている。国際標準規格 ITU-T Recommendation X.1142

- 政府機関統一基準に対応する項目：2.1.1.1～2.1.1.4
- 物理構成モデルのセグメントに対応する項目：S1～S6

5.14.統合ディレクトリ

5.14.1.統合ディレクトリの定義

統合ディレクトリは、各府省が個別に保有するアカウント情報のマスター・データベース機能を提供する。人事・給与情報システムや府省共通の職員等利用者共通認証基盤(GIMA)とデータ連携を行い、アカウント情報のマスター・データを保持する。統合ディレクトリに格納されたアカウント情報は、統合アカウント管理機能やディレクトリ連携機能により府省内の個別ディレクトリへ配布される。

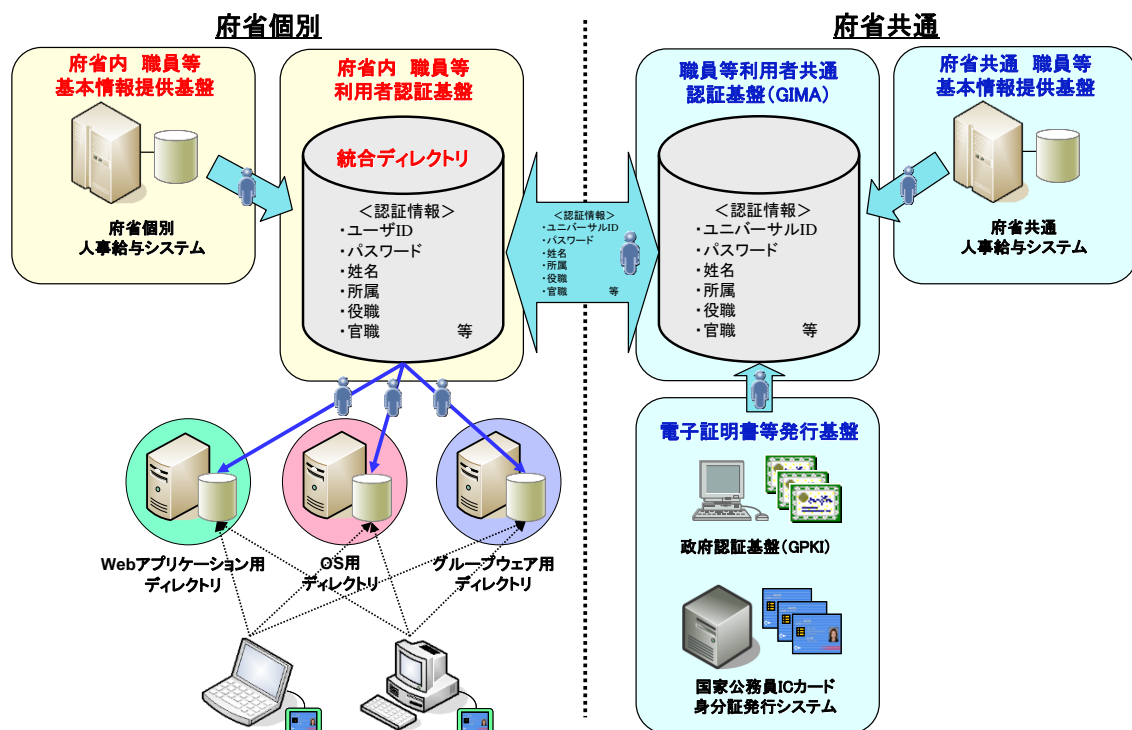



図 5.14-1 統合ディレクトリと職員等利用者共通認証基盤(GIMA)の関係

統合ディレクトリの機能・サービス	
機能・サービス	定義
統合ディレクトリ	府省ごとに構築されるアカウント情報のマスター・データベース機能を提供する。Web アプリケーションやグループウェアを利用する際のアカウント情報を一元的に管理するための基盤機能であるとともに、職員情報のディレクトリとして職員の検索にも対応する。 各種ディレクトリに格納するアカウント情報のマスターとなるデータを格納するため、人事異動の際には最新の組織・職員情報に更新する必要があり、人事給与システムや府省共通の職員等利用者共通認証基盤(GIMA)とデータ連携を行う。 [参考] 人事給与システムは、各府省が個別に構築したシステムと、業務・システム最適化計画に基づき府省共通で構築したシステムが存在する。現在は府省個別のシステムから、府省共通のシステムへ移行している段階であり、各府省の移行状況に応じて、統合ディレクトリが連携すべきシステムを選定する必要がある。 職員等利用者共通認証基盤(GIMA:Government Identity Management for Authentication)は、府省共通業務アプリケーション及び府省内業務アプリケーションを利用するためのアカウント情報を管理し、認証・認可・監査ログ取得機能を提供する。 ■職員等利用者共通認証基盤(GIMA)が提供する機能 ①アカウント情報の管理と提供 ②主体認証機能及び利用認可機能の提供 ③アクセス証跡情報(上記①、②に関するログ情報)の記録と提供 職員等利用者共通認証基盤(GIMA)は、人事給与システムの人事情報をオンラインにより取り込み、業務アプリケーションにおけるアカウント情報の管理業務を効率化する。 府省内のアカウント情報を一元的に管理する仕組みを既に保有している府省においては、既に保有しているこの仕組みを府省内職員等利用者認証基盤として活用し、府省内業務アプリケーションに対し、GIMA と同等の機能を提供する。 職員等利用者共通認証基盤(GIMA)とのデータ連携に必要な連携仕様書が整備されているので、必要に応じて参照すること。

5.14.2.統合ディレクトリの機能要件・非機能要件

機能要件 （認証情報としてパスワードを想定）		
1	基本	統合アカウント管理機能やディレクトリ連携機能と連携して、アカウント情報を一元的に管理する仕組みを実現すること。
2	基本	アカウント情報を保管し、一元的に管理するためのリポジトリ(データ保管)機能を提供すること。リポジトリには、利用者に関する次のような情報を格納できること。 ●Identifier ： 利用者を識別する ID(ユーザ ID 等) ●Credential ： 認証に使用するデータ(パスワード等) ●Common Profile ： 利用者に関するデータ(所属や官職等)
3	加点	リポジトリには、利用者に関する次のような情報を格納できること。 ●Application Profile ： アプリケーションが利用するデータ
4	加点	府省個別の人事給与システムとデータ連携が行えること。
5	基本	アカウント情報をインポート/エクスポートできる機能を有すること。
6	基本	外部システムとのデータ連携のインタフェースが提供されていること。
7	基本	アカウント情報に対する操作を、監査ログとして記録することができること。
8	加点	監査ログはレポートとしてわかりやすい形式で表示できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	認証を受けた管理者のみが、アカウント情報にアクセスできる仕組みを有すること。
	基本	管理者の役割や管理対象の範囲に応じて、適切なアクセス権を設定してアカウント情報を保護することができること。
	基本	取得した監査ログはアクセス制御を徹底して改ざんを防止すること。
	加点	通信の暗号化が可能なこと。
パフォーマンス	基本	「約 5 万」のアカウント情報を管理することとなり、人事異動の際には短期間に大量のユーザ属性を更新することが求められる。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とするシステムや利用者の増加に伴い、ユーザ ID の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	リポジトリに保管されたアカウント情報のデータのバックアップを取得すること。

関連する技術	
ディレクトリサービスアクセスプロトコル	LDAP:LDAP(Lightweight Directory Access Protocol)は、ディレクトリ・サービスに接続するために使用される標準プロトコル。LDAP V3 が規定されている。
ディレクトリサービスデータ交換形式	LDIF:LDIF(LDAP データ交換フォーマット：LDAP Data Interchange Format)は、LDAP のアカウント情報を交換する際に用いるファイル・フォーマットである。
データベースアクセス技術	JDBC:JDBC(Java Database Connectivity)は、Java プログラムから RDB へアクセスするための API。ディレクトリが RDB のケースでは利用が想定される。

・政府機関統一基準に対応する項目：2.1.1.1～2.1.1.4

・物理構成モデルのセグメントに対応する項目：S1～S6

5.15.WAN，省内 LAN, DNS/DHCP/Proxy，リモートアクセス

インターネットに接続する上で必要となる IPv4 グローバルアドレスは、新規に割り当て可能な在庫アドレス数が枯渇し、新規のアドレス割り当てができない状況である(新規割り当てのグローバルアドレスは IPv6 になる)。そのため、通常は新たな IPv4 グローバルアドレスを持ったサーバの増設や新たな DMZ の構築はできない。また、IPv6 は IPv4 と互換性がないため、単純には IPv6 と IPv4 のネットワークやサーバ間では通信できない。そのため、新たなアドレス割り当てや接続に対応するための IPv6 用環境と既存の IPv4 用環境の共存や併用の対策が必要となる。

この IPv4 と IPv6 の共存や併用が適切に行える様、インターネットに接続するネットワークやサーバ、PC 等の各種機器に関して、設計時及び機材調達時のみならず、運用・管理・監視・保守等の内容やセキュリティ対策についても、あらかじめ考慮しておくことが必要である。

なお、本節では主として IPv4 対応の観点から記載している。IPv6 化の対応を行う際には、設計・実装時にその旨考慮すること。

5.15.1.LAN

LAN とは、下図に示すように府省内で様々なサービスを提供するための基盤ネットワークである。

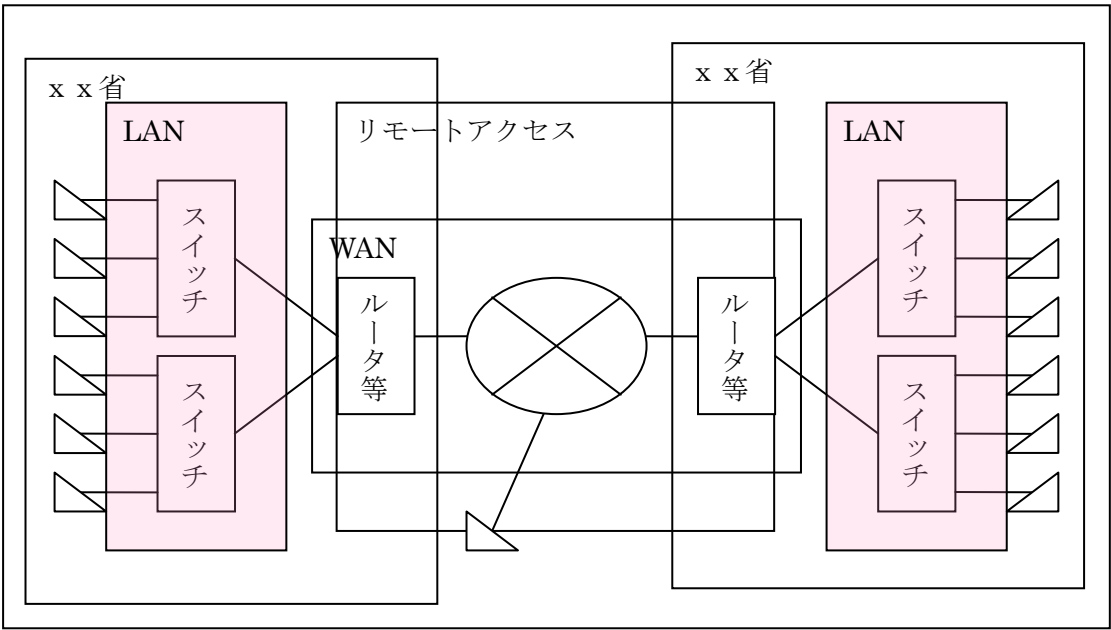



図 5.15-1 ネットワークにおける LAN の位置づけ

LAN の機能・サービスの定義は次の通りである。

機能・サービス	定義
レイヤー3 スイッチ	府省内にある複数のネットワーク(セグメント)を束ねる箇所にはレイヤー3 スイッチを配置する。本スイッチは、府省内 LAN のコアスイッチ(センタースイッ

	チ)の役割を担う。
レイヤー2 スイッチ	府省内の同一ネットワーク(セグメント)にあるネットワーク機器を束ねる箇所にはレイヤー2 スイッチを配置する。本スイッチは、府省内 LAN のフロアスイッチ(エッジスイッチ、アクセススイッチ)の役割を担う。
セキュア無線 LAN	無線 LAN とは、無線通信を利用してデータの送受信を行う LAN システムのことである。この無線 LAN のセキュリティを向上させたものがセキュア無線 LAN である。

5.15.1.1.レイヤー3 スイッチ

機能要件		
1	基本	DIX Ethernet Ver2 フレームによる通信ができること。また、IEEE802.3 フレームを利用している場合は、IEEE802.3 フレームによる通信ができること。
2	基本	ルーティング機能【Static,RIPv1/v2,OSPFv2/v3 等】を有すること。
3	基本	府省内でマルチキャストを利用したサービスを提供する場合、マルチキャストルーティング機能【PIM-SM/DM, IGMP 等】を有すること。
4	基本	同一ネットワーク(セグメント)内もしくは、異なるネットワーク(セグメント)間で中継されるパケットのアクセス制御を可能とする機能【アクセスコントロールリスト機能, フィルタリング機能　等】を有すること。
5	基本	府省内で提供される特定システムで送受信されるパケットを識別し、優先してパケット中継を行うことを可能とする優先制御機能【QoS　等】を有すること。
6	基本	IEEE802.1Q に準拠した VLAN 機能を有すること。
7	基本	IEEE802.3ad に準拠したリンクアグリゲーション機能を有すること。
8	基本	IEEE802.1D,IEEE802.1w, IEEE802.1s に準拠したスパニングツリープロトコル機能を有すること。
9	基本	府省内 LAN への不正接続防止等を目的として、ネットワーク認証機能【IEEE802.1X 認証, Web 認証, MAC アドレス認証　等】を有すること。
10	基本	ケーブルは、ポートに合わせた適切なタイプ【category5 等】を用意すること。
11	加点	セキュア無線 LAN(IEEE802.3af 方式でスイッチから受電する場合)に接続する場合又は接続予定があるスイッチは、IEEE802.3af に準拠した給電機能(POE)を有すること。

非機能要件		
性能	基本	府省内のサーバやネットワーク機器等を接続できる適切なタイプ【 10/100BASE-TX, 10/100/1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR, 10GBASE-LR 等】のポートを必要な数備えること。
	基本	府省内で提供されるサービスが必要とするスループットを十分に処理できる能力【バックプレーン性能, スイッチング性能　等】を有すること。
信頼性	基本	2 台以上のレイヤー3 スイッチで同一のデフォルトゲートウェイアドレスを共有し、障害時にはホットスタンバイによるネットワークの冗長化が可能となる機能【VRRP 等】を有すること。
	基本	物理ポートの故障に備え、運用に支障のない程度の予備ポートを有すること。
	基本	電源部の二重化や、電源の信頼性向上策【UPS　使用　等】を図ること。
セキュリティ	基本	管理者権限を使用するための識別認証機能を有すること。
	基本	管理者による ACL 等の設定、変更等の記録による監視(監査)に必要な機能を有すること。
運用保守	基本	設定情報の更新/動作状況の確認を行うためのコンソールポートを有すること。
	基本	運用管理端末からのリモート保守を可能とする機能【TELNET, SSH, Web 設定　等】を有すること。
	基本	構成定義情報のバックアップを可能とする機能【FTP, TFTP　等】を有すること。
	基本	運用管理サーバが府省内のネットワーク構成を運用/監視するために必要な機能【SNMP, RMON 等】を有すること。
	基本	レイヤー3 スイッチ内の時刻設定を常時正しい状態に保つことを可能とする機能【NTP 又は SNTP】を有すること。
	基本	レイヤー3 スイッチ上を流れるトラフィック解析を可能とする機能【ポートミラーリング　等】を有すること。
	基本	ログをサーバへ転送する機能【Syslog 等】を有すること。
	基本	19 インチラックにラックマウント可能であること。

関連する技術	
ルーティングプロトコル	RIP[Routing Information Protocol]は、レイヤー3 スイッチもしくはルータとの間で動的に経路交換を行うためのルーティングプロトコル。RIPv1:RFC1058、RIPv2:RFC2453 OSPF[Open Shortest Path First]は、レイヤー3 スイッチもしくはルータとの間で動的に経路交換を行うためのルーティングプロトコル。RIP のもつ問題点を改良したことで、大規模なネットワークにも利用できるルーティングプロトコル。OSPFv2/v3:RFC2328/RFC2740
ファイル転送プロトコル	FTP[File Transfer Protocol]は、ファイル転送用プロトコル。RFC959 TFTP[Trivial File Transfer Protocol]は、ファイル転送用プロトコル。RFC1350
マルチキャストプロトコル	PIM-SM[Protocol Independent Multicast- Sparse Mode]は、マルチキャストあてのパケットを中継するために必要な経路情報を作成するためのルーティングプロトコル。RFC2362 PIMーDM[Protocol Independent Multicast-Dence Mode]は、マルチキャストあてのパケットを中継するために必要な経路情報を作成するためのルーティングプロトコル。 IGMP[Internet Group Management Protocol]は、マルチキャストあてのパケットを受信するために構成されるマルチキャストグループを制御するためのプロトコル。IGMPv1:RFC1112、IGMPv2:RFC2236、IGMPv3:RFC3376
時刻同期プロトコル	NTP[Network Time Protocol]は、ネットワーク機器の内部時刻を外部サーバと同期をとることで常に正しい状態に保つためのプロトコル。NTPv3:RFC1305 SNTP[Simple Network Time Protocol]は、ネットワーク機器の内部時刻を外部サーバと同期をとれることで常に正しい状態に保つためのプロトコル。RFC1361
ネットワーク管理プロトコル	SNMP[Simple Network Management Protocol]は、ネットワーク機器をMIB(管理情報データベース)に基づいてネットワーク経由で監視・制御するためのプロトコル。SNMPv1、SNMPv2c、SNMPv3 の 3 つのバージョンをサポートする機器が一般的とされている。 RMON[Remote network Monitoring]は、遠隔地にあるネットワーク機器のトラフィックやエラー等の通信状況を監視するための MIB(管理情報データベース)。RFC1757。装置に実装されている MIB は、Ethernet Statistic、Ethernet History、Alarm、Event グループ の 4 グループが一般的である。 MIB[Management Information Base]は、ネットワーク管理プロトコルで使用するための管理情報の構造と識別方法を規格化したもの。RFC1213。標準的な定義と、ベンダー定義が存在する。
通信プロトコル	TELNET は、汎用的な双方向通信と仮想端末を提供するプロトコル。RFC854
暗号化通信プロトコル	SSH[Secure Shell]は暗号通信及び仮想端末を提供するプロトコル。ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、ほかのマシンへファイルを移動したりするためのプログラム。RFC4250-4256, 4716, 4819 SFTP[SSH File Transfer Protocol]は SSH を用いたファイル転送用プロ

	トコル。
ルータ冗長化プロトコル	VRRP[Virtual Router Redundancy Protocol]は、レイヤー3 スイッチやルータの冗長構成をとれるためのプロトコル。RFC2338
ログメッセージ転送プロトコル	Syslog は、ネットワーク機器のログメッセージを IP ネットワーク上で外部のサーバに転送するためのプロトコル。
リンク集約プロトコル	Link Aggregation は、複数の物理ポートを論理的に一つのポートとすることで、経路の冗長性を高め、広帯域を確保することができるプロトコル。IEEE802.3ad
仮想ネットワーク	VLAN[Virtual LAN]は、1 台のスイッチを複数のネットワークに分割することができる機能。VLAN には、ポートVLAN やタグVLAN、プロトコルVLAN といった方式がある。IEEE802.1Q
ループ回避プロトコル	STP[Spanning Tree Protocol]は、レイヤー2 における冗長構成をとれるためのプロトコル。STP には、RSTP や MSTP といった方式がある。IEEE802.1D,IEEE802.1w, IEEE802.1s
イーサネット通信規格	ネットワーク機器のもつイーサネットポートの標準規格。 10BASE-T:IEEE802.3、 100BASE-TX:IEEE802.3u、 1000BASE-T:IEEE802.3ab、 1000BASE-SX, 1000BASE-LX:IEEE802.3z、 10GBASE-SR, 10GBASE-LR:IEEE802.3ae
給電規格	POE[Power Over Ethernet]は、LAN ケーブルを利用して無線 LAN アクセスポイントや IP 電話等のネットワーク機器へ電源供給を行う方式。IEEE802.3af
認証規格	IEEE802.1X

5.15.1.2.レイヤー2 スイッチ

機能要件		
1	基本	IEEE802.3 フレーム及び DIX Ethernet Ver2 フレームによる通信ができること。
2	加点	同一ネットワーク(セグメント)内もしくは、異なるネットワーク(セグメント)間で中継されるパケットのアクセス制御を可能とする機能【アクセスコントロールリスト機能,フィルタリング機能 等】を有すること。
3	基本	府省内で提供される特定システムで送受信されるパケットを識別し、優先してパケット中継を行うことを可能とする優先制御機能【QoS 等】を有すること。
4	基本	IEEE802.1Q に準拠した VLAN 機能を有すること。
5	基本	IEEE802.3ad に準拠したリンクアグリゲーション機能を有すること。
6	基本	IEEE802.1D,IEEE802.1w, IEEE802.1s に準拠したスパニングツリープロトコル機能を有すること。
7	基本	府省内 LAN への不正接続防止等を目的として、ネットワーク認証機能【IEEE802.1X 認証, Web 認証, MAC アドレス認証 等】を有すること。
8	加点	セキュア無線 LAN(IEEE802.3af 方式でスイッチから受電する場合)に接続する場合又は接続予定があるスイッチは、IEEE802.3af に準拠した給電機能(POE)を有すること。
9	基本	ケーブルは、ポートに合わせた適切なタイプ【category5 等】を用意すること。

非機能要件		
性能	基本	府省内のサーバやネットワーク機器等を接続できる適切なタイプ【 10/100BASE-TX, 10/100/1000BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR, 10GBASE-LR 等】のポートを必要な数備えること。
	基本	府省内で提供されるサービスが必要とするスループットを十分に処理できる能力【バックプレーン性能, スイッチング性能 等】を有すること。
信頼性	基本	物理ポートの故障に備え、運用に支障のない程度の予備ポートを有すること。
セキュリティ	基本	管理者権限を使用するための識別認証機能を有すること。
	基本	管理者による ACL 等の設定、変更等の記録による監視(監査)に必要な機能を有すること。
運用保守	基本	設定情報の更新/動作状況の確認を行うためのコンソールポートを有すること。
	基本	運用管理端末からのリモート保守を可能とする機能【TELNET, SSH, Web 設定 等】を有すること。
	基本	構成定義情報のバックアップを可能とする機能【FTP, TFTP 等】を有すること。
	基本	運用管理サーバが府省内のネットワーク構成を運用/監視するために必要な機能【SNMP, RMON 等】を有すること。
	基本	レイヤー2 スイッチ内の時刻設定を常時正しい状態に保つことを可能とする機能【NTP, SNTP 等】を有すること。
	基本	レイヤー2 スイッチ上を流れるトラフィック解析を可能とする機能【ポートミラーリング 等】を有すること。
	基本	ログをサーバへ転送する機能【Syslog 等】を有すること。
	基本	19 インチラックにラックマウント可能であること。

関連する技術	
ファイル転送プロトコル	FTP[File Transfer Protocol]は、ファイル転送用プロトコル。RFC959 TFTP[Trivial File Transfer Protocol]は、ファイル転送用プロトコル。RFC1350
時刻同期プロトコル	NTP[Network Time Protocol]は、ネットワーク機器の内部時刻を外部サーバと同期をとることで常に正しい状態に保つためのプロトコル。NTPv3:RFC1305 SNTP[Simple Network Time Protocol]は、ネットワーク機器の内部時刻を外部サーバと同期をとれることで常に正しい状態に保つためのプロトコル。RFC1361
ネットワーク管理プロトコル	SNMP[Simple Network Management Protocol]は、ネットワーク機器をMIB(管理情報データベース)に基づいてネットワーク経由で監視・制御するためのプロトコル。SNMPv1、SNMPv2c、SNMPv3 の 3 つのバージョンをサポートする機器が一般的とされている。 RMON[Remote network Monitoring]は、遠隔地にあるネットワーク機器のトラフィックやエラー等の通信状況を監視するための MIB(管理情報データベース)。RFC1757。装置に実装されている MIB は、Ethernet Statistic、Ethernet History、Alarm、Event グループ の 4 グループが一般的である。 MIB[Management Information Base]は、ネットワーク管理プロトコルで使用するための管理情報の構造と識別方法を規格化したもの。RFC1213。標準的な定義と、ベンダー定義が存在する。
通信プロトコル	TELNET は、汎用的な双方向通信と仮想端末を提供するプロトコル。RFC854
暗号化通信プロトコル	SSH[Secure Shell]は暗号通信及び仮想端末を提供するプロトコル。ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、ほかのマシンへファイルを移動したりするためのプログラム。RFC4250-4256, 4716, 4819 SFTP[SSH File Transfer Protocol]は SSH を用いたファイル転送用プロトコル。
ログメッセージ転送プロトコル	Syslog は、ネットワーク機器のログメッセージを IP ネットワーク上で外部のサーバに転送するためのプロトコル。
リンク集約プロトコル	Link Aggregation は、複数の物理ポートを論理的に一つのポートとすることで、経路の冗長性を高め、広帯域を確保することができるプロトコル。IEEE802.3ad
仮想ネットワーク	VLAN[Virtual LAN]は、1 台のスイッチを複数のネットワークに分割することができる機能。VLAN には、ポート VLAN やタグ VLAN、プロトコル VLAN といった方式がある。IEEE802.1Q
ループ回避プロトコル	STP[Spanning Tree Protocol]は、レイヤー2 における冗長構成をとれるためのプロトコル。STP には、RSTP や MSTP といった方式がある。IEEE802.1D,IEEE802.1w, IEEE802.1s
給電規格	POE[Power Over Ethernet]は、LAN ケーブルを利用して無線 LAN アクセスポイントや IP 電話等のネットワーク機器へ電源供給を行う方式。IEEE802.3af
認証規格	IEEE802.1X

5.15.1.3.セキュア無線 LAN

セキュア無線 LAN 導入にあたっては、セキュリティ強度について十分注意が必要である。

機能要件		
1	基本	TCP/IP,UDP/IP による通信が可能であること。
2	基本	アクセスポイント(AP)、クライアントともに伝送方式として IEEE802.11g、IEEE802.11a(W52,W53,W56)をサポートすること。
3	加点	AP、クライアントともに伝送方式として IEEE802.11n をサポートすること。
4	基本	AP、クライアントともに暗号化方式として AES をサポートすること。なおクライアントはサプリカントを利用する方式でもよい。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
5	基本	AP、クライアントともに認証方式として WPA2、IEEE802.1x【EAP-FAST/TLS/TTLS/PEAP 等】をサポートすること。なお、クライアントはサプリカントを利用する方式でもよい。また、接続時には端末の MAC アドレスによる認証もサポートすること。
6	基本	AP は ESS-ID ステルス機能をサポートすること。
7	基本	VoWLAN を行う場合は、AP あたりに接続する端末の数等を制限できること。
8	基本	受電方式として AC 電源及び IEEE802.3af 方式をサポートすること。 又は相当するパワーインジェクターでの代用も可とする(この場合、スイッチ側の給電機能との整合性をとること)。
9	加点	DHCP 機能又は DHCP リレー機能をもつこと。

非機能要件		
信頼性	基本	リモート端末からネットワーク経由で AP の設定のメンテナンスが可能であること。
セキュリティ	基本	無線アクセスポイントの設定、監査記録管理者の識別認証が行えること。
	基本	アクセスポイントの利用開始、アクセスログ、終了等のセキュリティに関する監査ログがとれること。
運用保守	基本	SNMP を利用して AP が管理できること。
	基本	Syslog サーバと連携できること。

関連する技術	
無線 LAN 規格	IEEE802.11a(W52,W53,W56)、IEEE802.11b/g,n
無線 LAN 認証方式	WPA[Wi-Fi Protected Access]は、無線 LAN の認証方式の規格。IEEE802.11i WPA2[Wi-Fi Protected Access 2]は、無線 LAN の認証方式の規格。2002 年に発表された WPA の新バージョンで、より強力な AES 暗号に対応している。IEEE802.11i
標準暗号化方式	AES[Advanced Encryption Standard]は、アメリカ合衆国の新暗号規格(Advanced Encryption Standard) として規格化された共通鍵暗号方式。FIPS PUB 197 PEAP[Protected Extensible Authentication Protocol]は、PPP[Point to Point Protocol]に認証機能を追加した拡張プロトコルのうち、サーバとクライアントで相互認証を行うプロトコルのことである。IEEE802.1x
セキュリティプロトコル	TLS[Transport Layer Security]は、公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数等のセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。IEEE802.1x TTLS[Tunneled Transport Layer Security]は、PPP 認証で利用される EAP 認証プロトコルの一種である TLS[Transport Layer Security]のうち、鍵暗号方式によって保護されたユーザ名/パスワード情報によって認証を行う方式のことである。IEEE802.1x EAP-FAST は、一般に利用可能な IEEE 802.1x の EAP[Extensible Authentication Protocol]で、対称鍵アルゴリズムを使用して認証プロセスのトンネル化を実現する。IEEE 802.1x および IEEE 802.11i に準拠
無線 LAN 発見困難化	ESS-ID stealth は、ネットワークの識別子である ESS-ID を一定時間ごとに周囲に発信する「ビーコン信号」の一部を秘匿する機能である。 IEEE 802.11
給電規格	POE[Power Over Ethernet]は、LAN ケーブルを利用して無線 LAN アクセスポイントや IP 電話等のネットワーク機器へ電源供給を行う方式。IEEE802.3af
DHCP	DHCP[Dynamic Host Configuration Protocol]は、インターネットに一時的に接続するコンピュータに、IP アドレス等必要な情報を自動的に割り当てるプロトコル。RFC2131、RFC2132
ネットワーク管理プロトコル	SNMP[Simple Network Management Protocol]は、ネットワーク機器を MIB(管理情報データベース)に基づいてネットワーク経由で監視・制御するためのプロトコル。SNMPv1、SNMPv2c、SNMPv3 の 3 つのバージョンをサポートする機器が一般的とされている。
ログメッセージ転送プロトコル	Syslog は、ネットワーク機器のログメッセージを IP ネットワーク上で外部のサーバに転送するためのプロトコル。

5.15.2.WAN

WAN とは、「広域通信網」の略である。電話回線や専用線を使って、本省－出先機関や各省間等、地理的に離れた地点にあるコンピュータ同士を接続し、データをやり取りすることである。

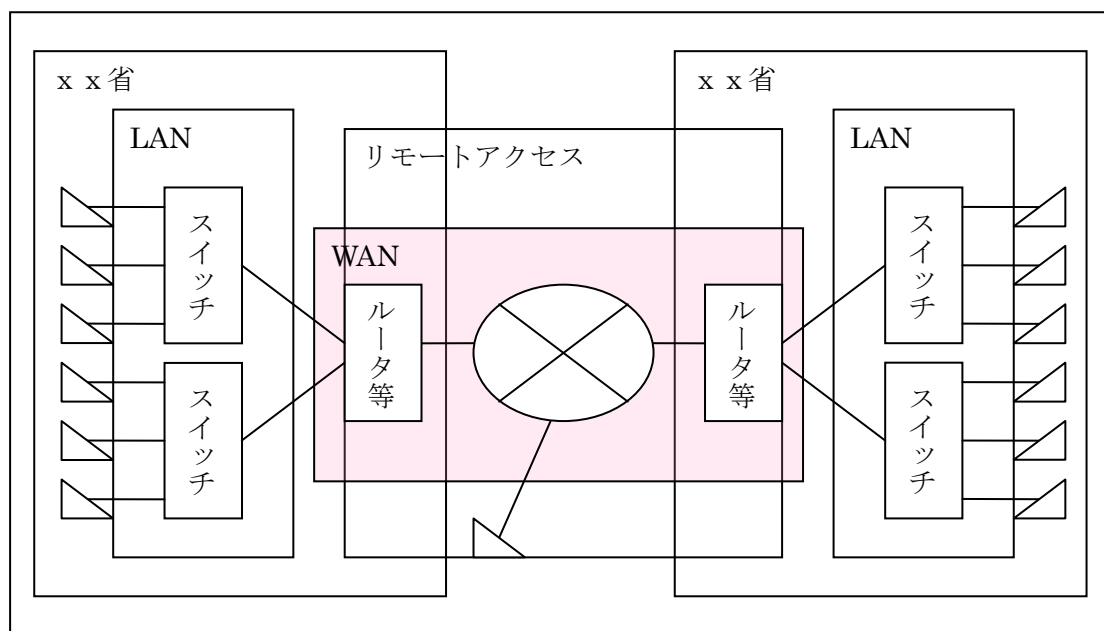



図 5.15-2 ネットワークにおける WAN の位置づけ

WAN の機能・サービスの定義は次の通りである。

機能・サービス	定義
ルータ	ルータとは、ネットワーク上を流れるデータをほかのネットワークに中継する機器である。
回線サービス （拠点間ネットワーク）	回線サービス（拠点間ネットワーク）とは、「広域通信網」のことである。電話回線や専用線を使って、本省－出先機関や各省間等、地理的に離れた地点にあるコンピュータ同士を接続し、データをやり取りすることである。 代表的な WAN としては、キャリア網を複数のユーザ企業で共有しその上でそれぞれ仮想的な LAN を構築する IP-VPN や広域イーサネット等がある。
回線サービス （インターネット接続）	回線サービス（インターネット接続）とは、インターネットプロトコル [Internet Protocol]技術を利用して、相互接続されたコンピュータネットワークである。 電話回線や専用線、接続事業者(ISP)を経由してインターネットへ接続し、インターネット上のコンピュータとデータ通信を実現する。

5.15.2.1.ルータ等

機能要件		
1	基本	DIX Ethernet Ver2 フレームによる通信ができること。また、IEEE802.3 フレームを利用している場合は、IEEE802.3 フレームによる通信ができること。
2	基本	ルーティング機能【Static,RIPv1/v2 等】を有すること。
	加点	ルーティング機能【OSPFv2/v3,BGP 等】を有すること。
3	基本	府省外でネットワーク接続する場合やインターネット VPN 接続を行う場合のルータの場合 IPsec(メインモード/アグレッシブモード)をサポートしていること。
	加点	上記以外の場合 IPsec(メインモード/アグレッシブモード)をサポートしていること。
4	基本	府省外でネットワーク接続やインターネット VPN 接続を行う場合のルータ 電子政府推奨暗号リストが公表された場合は、IPsec の暗号アルゴリズムに、リストに示された暗号強度を有するものを適用して各拠点間を相互接続できること。
	加点	上記以外の場合 電子政府推奨暗号リストが公表された場合は、リストに示された暗号強度を有するものを適用できること。
5	基本	ルータの場合 シェーピング機能を有すること。
	加点	SW の場合 シェーピング機能を有すること。
6	基本	府省内で提供される特定システムで送受信されるパケットを識別し、優先してパケット中継を行うことを可能とする優先制御機能【QoS 等】を有すること。
7	加点	ネットワークアドレスが重複しているネットワークに接続する場合は、NAT、NAPT 機能を有すること。
8	基本	同一ネットワーク(セグメント)内もしくは、異なるネットワーク(セグメント)間で中継されるパケットのアクセス制御を可能とする機能【アクセスコントロールリスト機能,フィルタリング機能 等】を有すること。
9	基本	ケーブルは、ポートに合わせた適切なタイプ【category5 等】を用意すること。

非機能要件		
性能	基本	府省内のサーバやネットワーク機器等を接続できる適切なタイプのポートを必要な数備えること。
	基本	府省内で提供されるサービスが必要とするスループットを十分に処理できる能力を有すること。
信頼性	基本	CPU 部の冗長化が可能であること。又は 2 台以上のルータを用意しOSPF/VRRP 等でネットワーク冗長化等を行うこと。
	加点	電源部の二重化や、電源の信頼性向上策【UPS 使用 等】を図ること。
	加点	物理ポートの故障に備え、運用に支障のない程度の予備ポートを有すること。
運用保守	基本	設定情報の更新/動作状況の確認を行うためのコンソールポートを有すること。
	基本	運用管理端末からのリモート保守を可能とする機能【TELNET, SSH, Web 設定 等】を有すること。
	基本	構成定義情報のバックアップを可能とする機能【FTP, TFTP 等】を有すること。
	基本	運用管理サーバが府省内のネットワーク構成を運用/監視するために必要な機能【SNMP 等】を有すること。
	基本	ルータ内の時刻設定を常時正しい状態に保つことを可能とする機能【NTP 又は SNTP】を有すること。
	基本	ログをサーバへ転送する機能【Syslog 等】を有すること。
	基本	19 インチラックにラックマウント可能であること。ただし、小規模であるなど、ラックマウントが必要でない場合などは除く。

関連する技術	
ルーティングプロトコル	RIP[Routing Information Protocol]は、レイヤー3 スイッチもしくはルータとの間で動的に経路交換を行うためのルーティングプロトコル。RIPv1:RFC1058、RIPv2:RFC2453 OSPF[Open Shortest Path First]は、レイヤー3 スイッチもしくはルータとの間で動的に経路交換を行うためのルーティングプロトコル。RIP のもつ問題点を改良したことで、大規模なネットワークにも利用できるルーティングプロトコル。OSPFv2/v3:RFC2328/RFC2740
ファイル転送プロトコル	FTP[File Transfer Protocol]は、ファイル転送用プロトコル。RFC959 TFTP[Trivial File Transfer Protocol]は、ファイル転送用プロトコル。RFC1350
時刻同期プロトコル	NTP[Network Time Protocol]は、ネットワーク機器の内部時刻を外部サーバと同期をとることで常に正しい状態に保つためのプロトコル。NTPv3:RFC1305 SNTP[Simple Network Time Protocol]は、ネットワーク機器の内部時刻を外部サーバと同期をとれることで常に正しい状態に保つためのプロトコル。RFC1361
ネットワーク管理プロトコル	SNMP[Simple Network Management Protocol]は、ネットワーク機器をMIB(管理情報データベース)に基づいてネットワーク経由で監視・制御するためのプロトコル。SNMPv1、SNMPv2c、SNMPv3 の 3 つのバージョンをサポ

	ートする機器が一般的とされている。 MIB[Management Information Base]は、ネットワーク管理プロトコルで使用するための管理情報の構造と識別方法を規格化したもの。RFC1213。標準的な定義と、ベンダー定義が存在する。
通信プロトコル	TELNET は、汎用的な双方向通信と仮想端末を提供するプロトコル。RFC854
暗号化通信プロトコル	SSH[Secure Shell]は暗号通信及び仮想端末を提供するプロトコル。ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、ほかのマシンへファイルを移動したりするためのプログラム。RFC4250-4256, 4716, 4819 SFTP[SSH File Transfer Protocol]は SSH を用いたファイル転送用プロトコル。
ログメッセージ転送プロトコル	Syslog は、ネットワーク機器のログメッセージを IP ネットワーク上で外部のサーバに転送するためのプロトコル。
イーサネット通信規格	ネットワーク機器のもつイーサネットポートの標準規格。 10BASE-T:IEEE802.3、 100BASE-TX:IEEE802.3u、 1000BASE-T:IEEE802.3ab、 1000BASE-SX, 1000BASE-LX:IEEE802.3z、 10GBASE-SR, 10GBASE-LR:IEEE802.3ae
暗号化通信規格	IPsec は、暗号化通信を行うための規格。RFC2401(Security Architecture for the Internet Protocol)、RFC2406(IP Encapsulating Security Payload [ESP])
鍵交換規格	IKE は、鍵交換を行うための規格。RFC2407(The Internet IP Security Domain of Interpretation for ISAKMP)、RFC2408(Internet Security Association and Key Management Protocol (ISAKMP))、RFC2409(The Internet Key Exchange (IKE))
ネットワークアドレス変換規格	NAT、NAPT は、アドレス変換を行うための規格。RFC1631(The IP Network Address Translator (NAT))

5.15.2.2.回線サービス(拠点間ネットワーク)

機能要件		
1	基本	IEEE802.3 フレーム及び DIX Ethernet Ver2 フレームによる通信ができること。
2	基本	バックボーンへのアクセス手段(アクセス回線)として、専用線、ATM、Ethernet、xDSL、FTTH をサポートしていること。
3	基本	システム間のトラフィックによる影響を最小限に抑えるため、【QoS(優先制御)機能等】を有すること。
4	基本	閉域性を確保し、外部ネットワークからのアクセスが不可能であること。
5	基本	ルータ監視をサービスの一環として提供できること。
6	基本	リモートアクセスをサービスの一環として提供できること。

非機能要件		
性能	基本	府省内で提供されるサービスが必要とするスループット(帯域)を確保できること。
信頼性	基本	冗長化等の最適な構成を構築し、予期せぬシステム停止【回線障害、ルータ障害　等】にも対応可能なネットワークであること。
	基本	耐障害性を向上させるため、メイン回線とバックアップ回線で利用する地域回線は、それぞれが異なる電気通信事業者が提供する地域回線を用いること。また、バックボーンについてもマルチキャリア対応(複数キャリアを用いた冗長構成)が可能なこと。 メイン回線とバックアップ回線の切り替えは自動で行われるものとする。
運用保守	基本	バックボーン回線・地域回線(アクセス回線)・終端装置に関し、障害発生時の問い合わせ窓口を設けること。
	基本	回線の保守監視・障害対応【障害発生通知、一次切り分け、障害報告　等】が可能なこと。
	基本	機器の修理・交換等に関し、オンサイト対応が可能なこと。
	基本	導入後、要望に応じて各回線のトラフィックデータを提供できること。

5.15.2.3.回線サービス(インターネット接続)

機能要件		
1	基本	IEEE802.3 フレーム及び DIX Ethernet Ver2 フレームによる通信ができること。
2	基本	プロバイダバックボーンスイッチは、IPv6 接続が可能であること。
3	基本	インターネットへのアクセス回線(インターネット接続対象拠点から ISP までの通信回線)として、専用線、ATM、Ethernet、FTTH をサポートしていること。
4	基本	ISP バックボーンは、国内主要 IX や海外主要 IX、海外主要 ISP と直接接続もしくはトランジットキャリアを介した接続が可能で、アクセス回線帯域以上の帯域が確保されていること。
5	基本	グローバル IP アドレスを必要数用意できること。
6	基本	DNS サーバをインターネット接続サービスの一環として提供できること。

非機能要件		
性能	基本	府省内で提供されるサービスが必要とするスループット(帯域)を確保できること。
信頼性	基本	冗長化等の最適な構成を構築し、予期せぬシステム停止【回線障害、ルータ障害　等】にも対応可能なネットワークであること。
	基本	耐障害性を向上させるため、メイン回線とバックアップ回線で利用する地域回線は、それぞれが異なる電気通信事業者が提供する地域回線を用いること。 また、メイン回線とバックアップ回線の切り替えは自動で行われるものとする。
	基本	必要に応じて、経路交換プロトコル(動的ルーティングプロトコル:BGP)を利用した冗長構成をとれること。
運用保守	基本	ISP・アクセス回線・終端装置に関し、障害発生時の問い合わせ窓口を設けること。
	基本	回線の保守監視・障害対応【障害発生通知、一次切り分け、障害報告　等】が可能なこと。
	基本	機器の修理・交換等に関し、オンサイト対応が可能なこと。

関連する技術	
経路交換プロトコル	BGP[Boarder Gateway Protocol]はレイヤー3 スイッチもしくはルータとの間で動的に経路交換を行うためのルーティングプロトコル。RFC4271

5.15.3.リモートアクセス

リモートアクセスとは、電話回線や専用線、インターネットを介して、外部ネットワークから内部ネットワーク(又はコンピュータ)に接続することである。

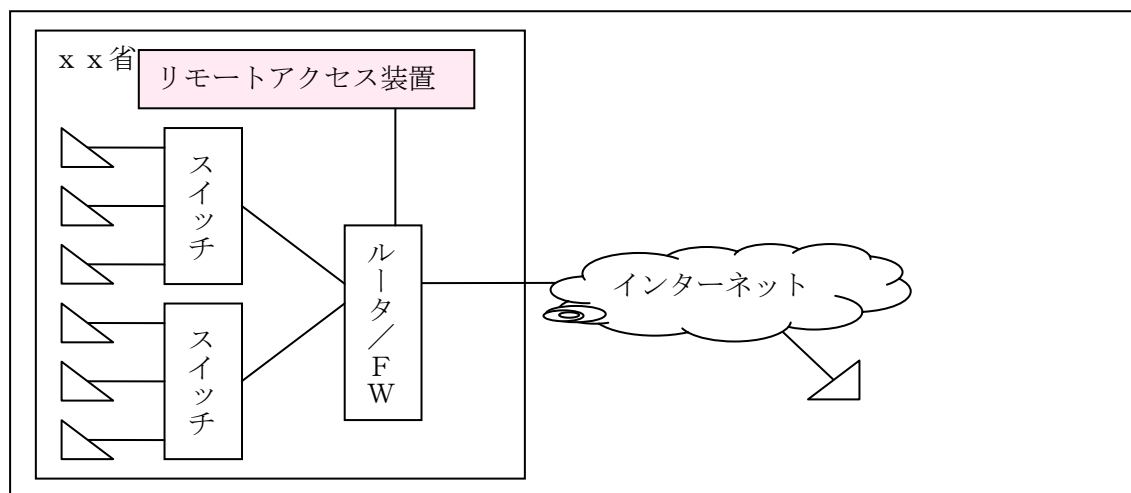



図 5.15-3 ネットワークにおけるリモートアクセス装置の配置

リモートアクセスの機能・サービスと定義は次の通りである。

機能・サービス	定義
リモートアクセス装置	リモートアクセス装置とは、電話回線や専用線、インターネットを介して、外部ネットワークから内部ネットワーク(又はコンピュータ)に接続するときに、アクセスの終端を行う装置のことである。

5.15.3.1.リモートアクセス装置

機能要件		
1	基本	IEEE802.3 フレーム及び DIX Ethernet Ver2 フレームによる通信ができること。
2	基本	不正端末の接続を防止する認証機能を有すること。
3	基本	認証サーバとの連携が可能であること。
4	基本	十分なセキュリティを確保するために、SSL や IPsec による暗号化通信機能を有すること。電子政府推奨暗号リストが公表された場合は、リストに示された暗号強度を有するものを適用すること。
5	基本	同時最大利用ユーザ数を定義できること。
6	基本	SSL 等による接続時に、Web アプリケーションが稼動可能なこと。
7	基本	ユーザ及びグループごとにアクセスレベルを設定でき、セキュリティポリシーの設定及びメンテナンスが容易であること。

非機能要件		
性能	基本	サービス提供範囲に位置するクライアントからの要求に対して応答できる性能【切断後の再接続ができること　等】を具備すること。
信頼性	基本	装置の冗長化が可能であること。
運用保守	基本	Web ブラウザあるいは CLI 経由での運用が可能であること。
	基本	【TELNET、FTP、SSH 等】により、遠隔からの保守機能をサポートすること。
	基本	運用管理サーバが府省内のネットワーク構成を運用/監視するために必要な機能【SNMP 等】を有すること。
	基本	19 インチラックにラックマウント可能であること。

関連する技術	
暗号化通信規格	IPsec は、暗号化通信を行うための規格。RFC2401(Security Architecture for the Internet Protocol)、RFC2406(IP Encapsulating Security Payload [ESP])
通信プロトコル	TELNET は、汎用的な双方向通信と仮想端末を提供するプロトコル。RFC854
ファイル転送プロトコル	FTP[File Transfer Protocol]は、ファイル転送用プロトコル。RFC959
暗号化通信プロトコル	SSH[Secure Shell]は暗号通信及び仮想端末を提供するプロトコル。ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、ほかのマシンへファイルを移動したりするためのプログラム。RFC4250-4256, 4716, 4819
ネットワーク管理プロトコル	SNMP[Simple Network Management Protocol]は、ネットワーク機器を MIB(管理情報データベース)に基づいてネットワーク経由で監視・制御するためのプロトコル。SNMPv1、SNMPv2c、SNMPv3 の 3 つのバージョンをサポートする機器が一般的とされている。

5.15.4.DNS/DHCP/Proxy

DNS とは IP アドレスとドメイン名やホスト名の関係を管理する機能である。

DHCP とはクライアントに対し使用すべき IP アドレスやサブネットマスクを配布したり、クライアントが使用すべきゲートウェイサーバ、DNS サーバ等の IP アドレスの通知を行う機能である。

Proxy とは内部ネットワークにあって外部ネットワークと直接通信ができない内部ネットワークのコンピュータに代わって通信を行う機能である。

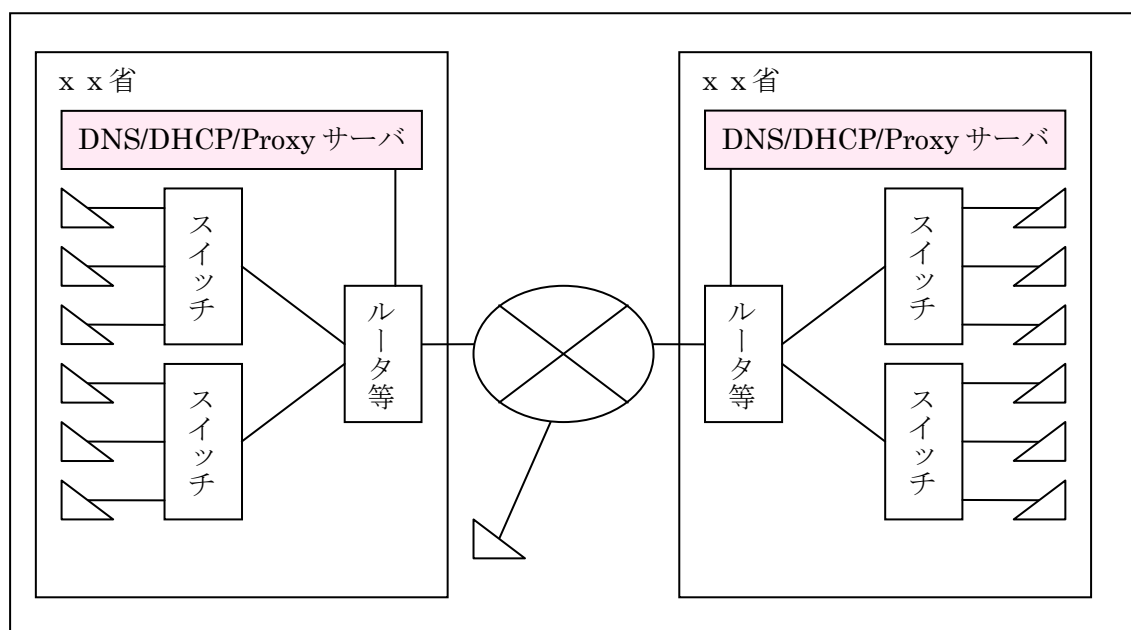



図 5.15-4 ネットワークにおける DNS／DHCP／Proxy サーバの配置

DNS/DHCP/Proxy の定義は次の通りである。

機能・サービス	定義
DNS サーバ	DNS サーバとは、IP アドレスとドメイン名やホスト名の関係を管理するサーバである。
DHCP サーバ	DHCP サーバとは、クライアントに対し使用すべき IP アドレスやサブネットマスクを配布したり、クライアントが使用すべきゲートウェイサーバ、DNS サーバ等の IP アドレスの通知を行うサーバである。
Proxy サーバ	Proxy サーバとは、内部ネットワークにあって外部ネットワークと直接通信ができない内部ネットワークのコンピュータに代わって通信を行うサーバである。

5.15.4.1.DNS サーバ

機能要件		
1	基本	TCP/IP による通信が可能であること。
2	基本	DNS プロトコルによる IP アドレスとドメイン名やホスト名間の名前(アドレス)解決機能を有すること。
3	基本	名前解決にあたっては、順引き及び逆引きに対応していること。
4	基本	上位又は下位の DNS サーバと連携する機能をもつこと。

非機能要件		
性能	基本	サービス提供範囲に位置するクライアントからの要求に対して応答できる性能を具備すること。
信頼性	基本	メインとサブの２台構成であるか、装置の冗長化が可能であること。
運用保守	基本	キャッシュのクリアが可能であること。
	基本	リモート装置からの保守が可能であること。
	基本	19 インチラックにラックマウント可能又は床置き対応であること。

関連する技術	
ドメインネームシステム	DNS[Domain Name System]は、インターネット上のホスト名や、電子メールに使われるドメイン名と IP アドレスとの対応付けを管理する。RFC1034、RFC1035

5.15.4.2.DHCP サーバ

機能要件		
1	基本	TCP/IP による通信が可能であること。
2	基本	DHCP プロトコルによる IP アドレス付与の機能を有すること。
3	基本	割り当てる IP アドレスの範囲が指定できること。

非機能要件		
性能	基本	サービス提供範囲に位置するクライアントからの要求に対して応答できる性能を具備すること。
信頼性	基本	装置の冗長化が可能であること。
運用保守	基本	リモート装置からの保守が可能であること。
	基本	19 インチラックにラックマウント可能又は床置き対応であること。

関連する技術	
DHCP	DHCP[Dynamic Host Configuration Protocol]は、インターネットに一時的に接続するコンピュータに、IP アドレス等必要な情報を自動的に割り当てるプロトコル。RFC2131、RFC2132

5.15.4.3.Proxy サーバ

機能要件		
1	基本	TCP/IP による通信が可能であること。
2	基本	インターネット及び省内の Web へのアクセスを Proxy サーバが中継できること。
3	基本	HTTP1.1 に対応した HTTP リクエストの中継機能を有すること。
4	基本	HTML コンテンツのキャッシュ機能を有すること。

非機能要件		
性能	基本	サービス提供範囲に位置するクライアントからの要求に対して応答できる性能を具備すること。
	基本	キャッシュ領域のサイズを変更できること、又は、業務に必要十分なキャッシュ領域を有していること。
信頼性	基本	装置の冗長化が可能であること。
運用保守	基本	リモート装置からの保守が可能であること。
	基本	19 インチラックにラックマウント可能又は床置き対応であること。

関連する技術	
代理サーバ	Proxy サーバは、企業等の内部ネットワークとインターネットの境にあって、直接インターネットに接続できない内部ネットワークのコンピュータに代わって、「代理」としてインターネットとの接続を行う。
ハイパーテキスト転送プロトコル	HTTP[Hyper Text Transfer Protocol]1.1。RFC2068
Web ページ記述言語	HTML「HyperText Markup Language]は、Web ページを記述するためのマークアップ言語。

5.15.5.VoIP

VoIP とは、下図に示すように府省内で様々な電話サービスを IP ネットワーク上で提供する基盤である。

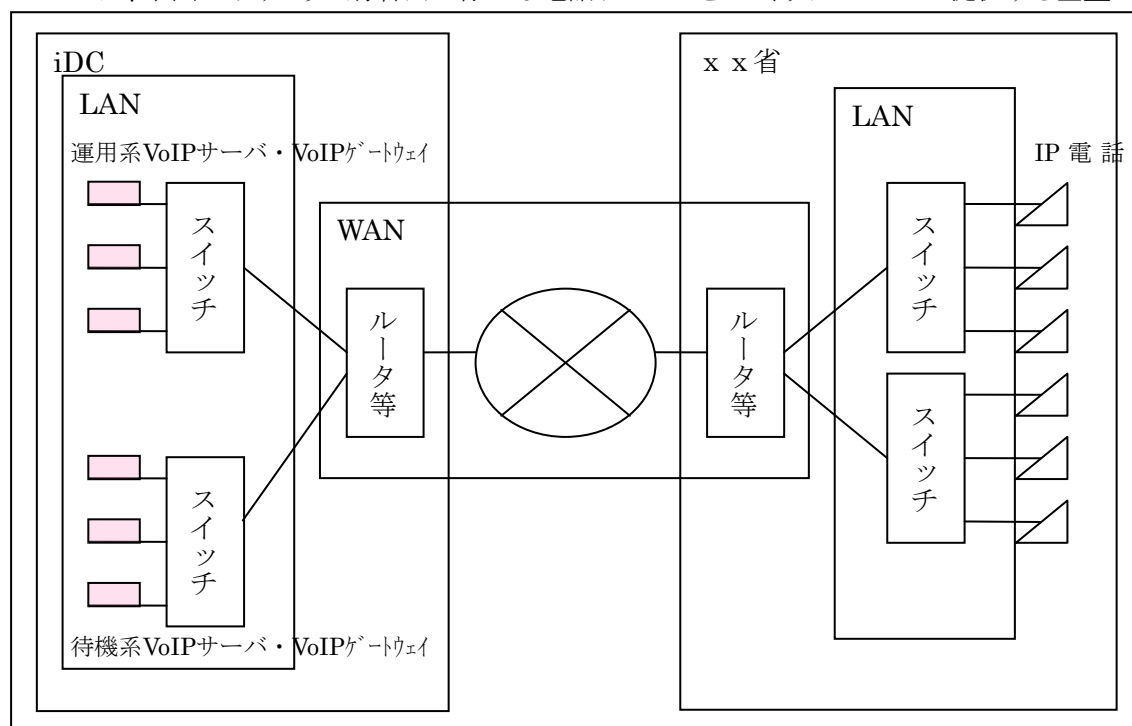



図 5.15-5 ネットワークにおける VoIP サーバ･VoIP ゲートウェイの配置

VoIP の機能･サービスと定義は次の通りである。

機能･サービス	定義
VoIP サーバ・VoIP ゲートウェイ	府省内にある複数のネットワーク(セグメント)を束ねるレイヤー3 スイッチに VoIP サーバ又は VoIP ゲートウェイとの組み合わせを配置する。VoIP サーバ･VoIP ゲートウェイは、府省内の様々な電話サービスを提供する役割を担う。

5.15.5.1.VoIP サーバ･VoIP ゲートウェイ

機能要件		
1	基本	府省内での内線相互接続機能、一般公衆網･IP 公衆網との外線接続機能を有すること。
2	基本	保留･転送･コールピックアップ機能を有すること。
3	基本	外線発信した際に送出する発信通知番号を内線単位で規定することのできる機能を有すること。
4	基本	モバイル端末【無線 LAN 電話端末、PHS 等】を接続できる機能を有すること。
5	基本	外線通話の通話料金削減のために最適方路選択機能【ARS 等】を有すること。
6	基本	府省内にある内線･部署単位で外線通話に関する課金(みなし課金)情報を帳票化し、出力する機能を有すること。
7	基本	府省内 LAN への不正接続防止等を目的として、IP 電話機にネットワーク認証機能【IEEE802.1x 認証, MAC アドレス認証 等】を有すること。
8	基本	IP 電話機の制御プロトコルは SIP(IETF RFC3261) に準拠していること。

非機能要件		
性能	基本	府省内に必要なIP電話機台数を収容できること。なお、IP電話機の増設に備え、収容が可能な最大容量も考慮すること。
	基本	府省内で提供される電話サービスが十分に処理できる能力【HCS、BHCA等】を有すること。
信頼性	基本	VoIPサーバが冗長化構成可能であること。
	基本	VoIPサーバ障害時、バックアップ側VoIPサーバに業務に支障ない時間内に切り替わること。
	基本	VoIPサーバ障害時、バックアップ側VoIPサーバに切り替わった際の通話中の呼が接続断を起こさないこと。
運用保守	基本	設定情報の更新/動作状況の確認を行うためのログを有すること。
	基本	運用管理端末からのリモート保守を可能とする機能【TELNET, SSH, Web設定等】を有すること。
	基本	構成定義情報のバックアップを可能とする機能【FTP, TFTP 等】を有すること。
	基本	VoIPサーバは運用管理サーバと連携し、VoIPサーバ上で動作しているプロセスを監視することができること。
	基本	ログをサーバへ転送する機能【Syslog 等】を有すること。
	基本	19インチラックにラックマウント可能又は床置き対応であること。

関連する技術	
IP電話等プロトコル	SIP[Session Initiation Protocol]は、IP 電話機等の制御プロトコル。IETF RFC3261
認証規格	IEEE802.1X
ファイル転送プロトコル	FTP[File Transfer Protocol]は、ファイル転送用プロトコル。RFC959 TFTP[Trivial File Transfer Protocol]は、ファイル転送用プロトコル。RFC1350
ログメッセージ転送プロトコル	Syslogは、ネットワーク機器のログメッセージをIPネットワーク上で外部のサーバに転送するためのプロトコル。

5.16.ワークフロー、BAM

5.16.1.ワークフロー、 BAM の定義

ワークフローとは、ビジネスプロセス全体あるいはその一部における、確実な反復可能性を持つ一連の作業パターンであり、これによってドキュメント・情報・タスクが、既定の処理手順に従って，担当者から担当者へ円滑に引き継がれるものである。ワークフローは作業の内容や順番などを吟味して業務流れ図などで表されることが多い。

このワークフローを IT システム上に定義し，生成し，運用するために特化したソフトウェアをワークフロー管理システムと呼ぶ。これにより、作業担当の自動割り振りや順序などの実行制御、ワークフローに伴う情報/データの管理と伝達、進捗状況のモニタリングなどが可能になる。

ワークフロー管理システムを用いることで、申請書、稟議書、交通費の精算、休暇届や引っ越し届など、これまで省内の各部門や担当者間を巡回していた書類を電子データ化し、効率的に処理することができ、回覧処理の平行化や、出張先からのノート PC を利用した決裁など、業務スピード向上を期待できる。

BAM(Business Activity Monitoring)とは、業務処理の実施状況や実績をリアルタイムにモニタリングし、異常値等に対してアラートを発して管理者や担当者の意思決定や問題への対応等の次のアクションのトリガーとする一連のテクノロジやプロセスを表す。また、組織の重要な業績評価指標(KPI)の達成度に結びついた業務処理をモニタリングし、実行状況や KPI を可視化し、ダッシュボード画面上に表示したりする。

モニタリングによるアラートにより、業務プロセス上の機会や問題に対して迅速に対応し、業務プロセス効率を向上させることが BAM の目的である。また、計測・蓄積されたモニタリングデータは、業務プロセスの見直し、再設計にも有効な情報となる。

5.17.ドメイン共通

5.17.1.定義

ドメイン共通とは、通信プロトコル、データフォーマット、文字コード等の複数の技術ドメインに共通する要件の集合である。本章には関連する技術だけが存在し、機能要件、非機能要件は存在しない。機能要件及び非機能要件は関連する技術ドメインで示される。

関連する技術	
通信プロトコル	IP: IETF RFC 791 TCP: IETF RFC 793 UDP: IETF RFC 968 HTTP 1.1: IETF RFC 2616 HTTP over TLS: IETF RFC 2818 TLS: IETF RFC 4243 FTP: IETF RFC 959 FTPS: IETF RFC 2229 SSH: IETF RFC 4250, 4251, 4252, 4253, 4254, 4255, 4256
国際符号化文字集合	Unicode: ISO/IEC 10646
グラフィックフォーマット	JPEG: ISO/IEC 15444-1, -2, -3 PNG: ISO/IEC 15948

6.役務調達

本章では、情報システム調達において調達すべき“役務”をこれまで公開された府省の情報システムの調達仕様書をもとに整理し、仕様書への記載方法を解説している。“物品”の調達については本章の対象ではないことから第５章を参照すること。

本章では、情報システムに関連する役務を、情報システムのフェーズから分類した。

図 6.－１ 役務調達の分類

表 6.-1 各役務に関する説明

役務	対象とする役務作業
6.1 全体計画策定支援	システム化構想の立案、システム化計画の立案
6.2 調達支援	要件定義の実施、調達方針・調達方式決定、調達仕様書の作成、意見招請、受注者の評価、プロジェクト管理などの府省の調達業務を支援する役務作業
6.3 システム構築（設計・開発）	情報システムの設計、開発、移行、運用・保守設計などの情報システムの構築に係わる役務作業
6.4 運用	情報システムの運用業務に係わる役務作業 （6.5 ヘルプデスクは 6.4 の作業の一部に位置づけられるが、本章では分けて記載を行っている）
6.5 ヘルプデスク	システム運用業務における利用者からの問い合わせに対応するヘルプデスク業務にかかわる役務作業
6.6 保守	情報システムの障害の訂正、納入後のシステム・ソフトウェア製品の修正、変更された環境への適合など、情報システムの保守を行う役務作業
6.7 機器調達付帯作業	情報システムに必要な機器（ハードウェアと不可分な OS 等の既製のソフトウェアを含む）の設置・設定等、機器調達に付帯して発生する役務作業 （※保守は含まない）
6.8 iDC 設備調達付帯作業	受注者が用意する施設（データセンター）への各種機器の設置、設定、対象システムの運用監視（及びそれに付帯する業務）、などの役務作業
6.9 ネットワーク調達	LAN、WAN 等の構内ネットワークの構築に関わる役務、WAN 等の広域ネットワークサービスやインターネットサービス等のサービスの調達に付随する役務作業
6.10 クラウドサービス	クラウドシステムのサービスを利用する役務作業
6.11 クラウド構築	クラウドシステムを構築する役務作業
6.12 セキュリティ	本節では各役務の調達におけるセキュリティの留意点、情報システムの構築時におけるセキュリティの検討方法を記載
6.13 その他（作成予定）	業務パッケージソフトウェアの調達など、6.1～6.12 に分類されない役務作業

6.1.全体計画策定支援

6.1.1.調達分野の定義

全体計画策定支援とは、システムの構築・運用に係る全体計画を発注者が決定する際に、本作業の受注者が発注者側の作業を支援する事を指す。

なお、全体計画策定にあたって業務プロセス・制度・組織等の改革を検討する場合は本工程において検討を行う。

図　6.1-1　役務調達の分類における対応箇所

6.1.2 仕様書に記載すべき役務内容

6.1.2.1.代表的な役務作業の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [1]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務作業の概要	共通フレーム 2007 の アクティビティ	調達基本指針[2]に対応する仕様書の章・節 （及びそのタイトル）
1. システム化構想の立案	現行システムの課題抽出（※現行システムが存在する場合） システム化要望の調査 技術動向の調査 システム化構想書の作成　等	1.4.2 システム化構想の立案	－
2. システム化計画の立案	システムの概要検討 設計・開発・移行・運用スケジュールの策定 概算見積もりの実施 システム化計画書の作成　等	1.4.3 システム化計画の立案	－

1 独立行政法人　情報処理推進機構　共通フレーム 2007
ソフトウェアライフサイクルプロセス　SLCP-JCF 2007
2 総務省　情報システムに関わる政府調達の基本指針　2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

6.1.2.2.各役務内容に関する説明及び仕様書上の記載例

1. システム化構想の立案

項目	内容
役務内容の概要	システム構築を進めるにあたって、システム化要望の調査、技術動向の調査等を行い、システム化構想を策定する。現行システムが存在する場合は、現行システムの課題を抽出する。
想定されるインプット （発注者側で用意）	既存システムの要件定義書、設計書等（※既存システムが存在する場合） システム化にあたっての発注者側の要望事項 前回の最適化計画に係る資料がある場合は、当該資料一式
成果物 （受注者側で用意）	システム化構想書
仕様書に記載すべきポイント	システム化構想の立案の要求事項を記載する。 **【1.基本的に記載すべき要件】** ・ システム化要望の調査 ・ 技術動向の調査 ・ システム化構想の策定　等 **【2.案件の種類・特性によって追記すべき要件】** ●既存システムが存在する場合 ・ 現行システムの課題抽出　等
仕様書記載上の例/説明	**【1.基本的に記載すべき要件】** (1)システム化要望の調査 関係者に対するヒアリング等により、システム化に対する要望を調査すること。 (2)技術動向の調査 国内外の最新技術動向の調査を行い、適用可能性の検討及び適用する場合の課題について整理を行うこと。 (3)システム化構想の策定 システム化要望の調査や技術動向の調査の結果を踏まえ、新システムの全体像・システム構築方針・概算費用・想定される効果の概要等を明確にしたシステム化構想書を作成すること。 **【2.案件の種類・特性によって追記すべき要件】** ●既存システムが存在する場合 (1)既存システムの課題抽出 既存システムの利用者に対するヒアリング等により既存システムの問題点を調査し、解決すべき課題を整理すること。
案件・情報システムの特性等による留意点	―
セキュリティに関する	重要な情報の取り扱う情報システムの場合、システム化構想にセ

留意点	キュリティに関する構想を含める。

2. システム化計画の立案

項目	内容
役務内容の概要	システム化構想書を踏まえ、システムの将来像を具体化し、概算見積もりを行ったうえで、設計・開発・運用スケジュールを策定する。これらの内容を、システム化計画書として取りまとめる。
想定されるインプット （発注者側で用意）	システム化構想書 既存システムの要件定義書、設計書等（※既存システムが存在する場合） システム化にあたっての発注者側の要望事項
成果物 （受注者側で用意）	システム化計画書 最適化計画（※最適化対象システムの場合）
仕様書に記載すべきポイント	システム化計画の立案の要求事項を記載する。 **【1.基本的に記載すべき要件】** ・ システムの概要検討 ・ 設計・開発・運用スケジュールの策定 ・ 概算見積もりの実施 ・ システム化計画書の作成 **【2.案件の種類・特性によって追記すべき要件】** ●最適化対象のシステムの場合 ・ 最適化計画の策定
仕様書記載上の例/説明	**【1.基本的に記載すべき要件】** (1)システムの概要検討 システムが備えるべき基本的な機能要件を整理した上で、システム機能構成図を作成すること。また、大まかなシステム構成を検討し、ハードウェア構成図、ソフトウェア構成図、ネットワーク構成図を作成すること。 (2)設計・開発・運用スケジュールの策定 システム構築に要する期間を検討した上で、システム開発・運用にあたっての全体スケジュールを策定すること。 (3)概算見積もりの実施 システム構築に要する費用について、概算で見積もりを行うこと。 (4)システム化計画書の作成 システムの将来像や設計・開発・運用スケジュール、概算見積もり結果を整理したシステム化計画書を作成すること。システム化計画書には、発注者側と受注者側の体制と役割、制約条件及び前提条件、遵守すべき標準管理要領等についても定義すること。

	【2.案件の種類・特性によって追記すべき要件】 ●最適化対象のシステムの場合 (1)最適化計画の策定 「業務・システム最適化計画　ガイドライン」に基づき、対象となる業務・システムの概要、最適化の実施内容、最適化工程表、現行体系及び将来体系、最適化効果指標・サービス指標一覧を定義した「最適化計画」を策定すること。
案件・情報システムの特性等による留意点	「業務・システム最適化計画　ガイドライン」に定義された、業務・システム最適化対象のシステムについては、最適化計画を策定する。
セキュリティに関する留意点	重要な情報の取り扱う情報システムの場合、システム化計画にセキュリティに関する検討を含める。

6.1.3.納入成果物と提出のタイミング

代表的な納入成果物とタイミングを記載すると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。

役務	納入成果物	納入期限
1. システム化構想の立案	システム化構想書	プロジェクト完了時
2. システム化計画の立案	システム化計画書 最適化計画	プロジェクト完了時

6.1.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務	インプット	インプットを提示するタイミング
1. システム化構想の立案	既存システムの要件定義書、設計書等	入札公示時
	システム化にあたっての発注者側の要望事項	入札公示時
2. システム化計画の立案	システム化構想書	入札公示時
	既存システムの要件定義書、設計書等	入札公示時
	システム化にあたっての発注者側の要望事項	入札公示時

6.1.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。
調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表を作成することが必要である。

6.2.調達支援

6.2.1.調達分野の定義

調達支援とは、設計・開発時における発注者側の作業の支援を指す。本文書では「6.2.2. 要件定義段階における調達支援」、「6.2.3. プロジェクト管理など設計・開発以降における調達支援」の 2 つの役務を対象とする。

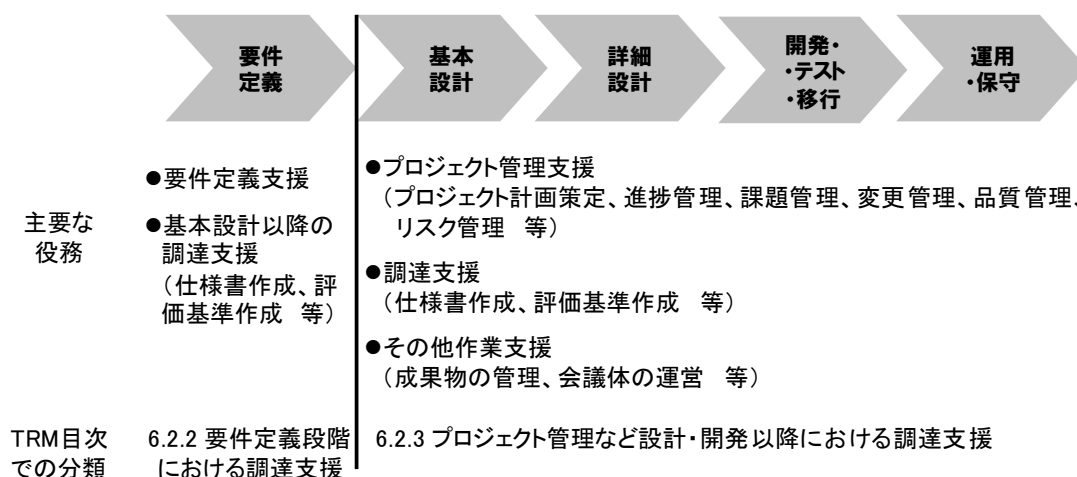



図 6. 2-1 調達支援における役務分類

役務分類	対象とする役務作業
6. 2. 2 要件定義段階における調達支援	要件定義の実施、基本設計以降の物品･役務の調達 （調達方針･調達方式決定支援、調達仕様書の作成、意見招請の支援、受注者の評価）などの役務作業支援
6. 2. 3 プロジェクト管理など設計･開発以降における調達支援	システム開発に関わるプロジェクト管理、及び物品･役務の調達 （調達方針･調達方式決定支援、調達仕様書の作成、意見招請の支援、受注者の評価）などの役務作業支援

6.2.2.要件定義段階における調達支援

6.2.2.1.調達分野の定義

本項で指す、「要件定義段階における調達支援」は要件定義、及びそれに基づくシステムの設計・開発の調達仕様書の作成支援など要件定義段階における支援業務を指す（図 6.2-1 及び図 6.2-2 参照）。尚、設計・開発業務（システム構築業務）以降のプロジェクト等に関する調達支援業務は本項の対象には含まれていないため、当該領域における役務については 6.2.3 の項を参照のこと。

図 6. 2-2 情報システムの工程における本役務の範囲

6.2.2.2.仕様書に記載すべき役務内容

6.2.2.2.1.代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [3]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[4]の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務作業の概要	共通フレーム 2007 のアクティビティ	調達基本指針に対応する仕様書の章・節（及びそのタイトル）
1. 最適化計画の確認・評価・改善・効果算定	最適化計画の確認、評価及び改善提案、最適化効果の算定の支援	1.4.3 システム化計画の立案	3. 情報システムの要件 4. 規模・性能要件 5. 信頼性等要件 6. 情報セキュリティ要件 7. 情報システム稼働環境 8. テスト要件定義 9. 移行要件定義」 10. 運用要件定義 11. 保守要件定義
2. 要件定義の支援	以下の点に関する要件定義の支援 ・スケジュール定義 ・業務・機能要件定義 ・システム方式要件定義 ・情報・データ要件定義 ・ユーザインタフェース要件定義 ・外部インタフェース要件定義 ・ネットワーク要件定義 ・ソフトウェア要件定義 ・ハードウェア要件定義 ・情報セキュリティ要件定義 ・設計・開発要件定義 ・テスト要件定義 ・移行要件定義 ・運用・保守要件定義	1.5.2.4 機能要件の定義 1.5.2.5 非機能要件の定義 1.6.2 システム要件定義 1.5.2.6 スケジュールに関する要件の定義	
3. システムコストの試算	2において実施した要件定義に基づいたシステムの構築・運用コストの試算	1.5.2.5 非機能要件の定義	
4. 調達業務の支援	調達計画書の作成、調達仕様書の作成、意見請招対応、事業者の評価等、調達関連業務の支援	1.1.2 提案依頼書の準備 1.1.3 契約準備及び更新	

[3] 独立行政法人　情報処理推進機構　共通フレーム 2007
ソフトウェアライフサイクルプロセス　SLCP-JCF 2007

[4] 総務省　情報システムに関わる政府調達の基本指針　2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

6.2.2.2.2.各役務内容に関する説明及び仕様書上の記載例

1. 最適化計画の確認･評価･改善･効果算定

項目	内容
役務作業内容の概要	作成された最適化計画を確認・評価し、必要があれば改善提案を行う。また、最適化効果の試算を支援する。
想定されるインプット （発注者側で用意）	・最適化計画
成果物 （受注者側で用意）	・最適化計画の確認・評価・改善・効果算定に関する報告書
仕様書に記載すべきポイント	【1.基本的に記載すべき要件】 ・最適化計画の確認・評価・改善提案 ・計画実施時における効果の算定
仕様書記載上の例/説明	○最適化計画の確認・評価及び改善提案 当省が提示する最適化計画について、「情報システムに係る政府調達の基本指針」、「業務・システム最適化指針」、「○○省情報ネットワーク（共通システム）最適化計画」との整合性等に関し、確認・評価及び改善提案を行うこと。 ○計画実施時における効果の算定 計画を実現した場合の経費削減や業務処理時間短縮等の効果について、最適化計画で算出された内容を確認し、必要に応じて見直しを行うこと。
案件・情報システムの特性等による留意点	「6.1 全体計画策定支援」において、最適化計画を策定した場合のみ本作業が必要となる。
セキュリティに関する留意点	－

2. 要件定義の支援

項目	内容
役務作業内容の概要	調達対象となるシステム、業務に係る要件定義を支援する。
想定されるインプット （発注者側で用意）	・システム化計画書 ・最適化計画（※最適化計画が存在する場合） ・既存システムの要件定義書、設計書等（※既存システムが存在する場合） ・その他受注者の必要に応じて提示する情報
成果物 （受注者側で用意）	・要件定義書
仕様書に記載すべきポイント	【1.基本的に記載すべき要件】 以下の内容について、要件定義を支援する。 ・スケジュール定義 ・業務・機能要件定義 ・システム方式要件定義 ・情報・データ要件定義 ・ユーザインタフェース要件定義 ・外部インタフェース要件定義 ・ネットワーク要件定義 ・ソフトウェア要件定義 ・ハードウェア要件定義 ・情報セキュリティ要件定義 ・設計・開発要件定義 ・テスト要件定義 ・移行要件定義 ・運用・保守要件定義
仕様書記載上の例/説明	○要件定義の実施 当省の「最適化計画案」・当省が別途提示するガイドライン等及び当省との協議結果に基づき、下記の要件を定義し、要件定義書として、取りまとめること。 A) スケジュール定義 B) 業務・機能要件定義 C) システム方式要件定義 D) 情報・データ要件定義 E) ユーザインタフェース要件定義 F) 外部インタフェース要件定義 G) ネットワーク要件定義 H) ソフトウェア要件定義

項目	内容
	I) ハードウェア要件定義 J) 情報セキュリティ要件定義 K) 設計・開発要件定義 L) テスト要件定義 M) 移行要件定義 N) 運用・保守要件定義
案件・情報システムの特性等による留意点	組織変更が発生する場合は、その影響についても要件定義にて検討する。
セキュリティに関する留意点	発注者及び仕様書作成者は、「政府機関の情報セキュリティ対策のための統一基準」及び各府省の情報セキュリティポリシーに準拠して、情報セキュリティ要件の定義を行うこと。特に以下の要件に関しては、総務省　情報システムに係る政府調達の基本指針において仕様書への記載が求められている事から、特に明確に定義を行うこと （１）　権限の定義 （２）　セキュリティ対策の定義

3．システムコストの試算

項目	内容
役務作業内容の概要	要件定義の結果から、システムの構築・運用に掛かるコストを試算する。
想定されるインプット （発注者側で用意）	・要件定義書 （2 の成果物）
成果物 （受注者側で用意）	・システム構築経費積算書（案） ・運用経費積算書（案）
仕様書に記載すべきポイント	【1.基本的に記載すべき要件】 ・コストの試算及び経費積算書の作成
仕様書記載上の例/説明	○コストの試算及び経費積算書の作成 ・要件定義書に基づき、定義されている各種機能及び役務、システム構築及び運用経費等のコストの積算を行い、経費積算書案として取りまとめること。 ・積算項目や積算方法及び積算の類型については当課担当職員の了解を得ること。
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	―

4. 調達業務の支援

項目	内容
役務作業内容の概要	調達計画書の作成、調達仕様書の作成、意見請招対応、事業者の評価等、設計・開発の調達に係わる業務の支援を行う。
想定されるインプット （発注者側で用意）	・最適化計画（※最適化計画が存在する場合） ・要件定義書 （2 の成果物）
成果物 （受注者側で用意）	・調達計画書（案） ・調達仕様書（案） ・応札資料作成要領（案） ・評価手順書（案） ・評価項目一覧（案） ・評価基準書（案） ・評価採点表（案） ・意見招請回答管理表 ・入札公示に係わる説明資料（案） ・入札公示後に必要となる予算根拠となる説明資料（案）
仕様書に記載すべきポイント	**【1.基本的に記載すべき要件】** ・調達方法・方式の策定支援 ・調達仕様書（案）、応札資料作成要領（案）、評価手順書、評価項目一覧等の調達手続きに係わる資料の作成支援 ・意見招請への対応支援 ・応札事業者の評価支援 **【2.案件の種類・特性によって追記すべき要件】** （特定情報システム（設計・開発の予定価格が 5 億円を超えるもの）に当たる案件） ・調達計画書（案）の作成支援 ・政府全体管理組織及び府省全体管理組織の指摘事項対応支援
仕様書記載上の例/説明	**【1.基本的に記載すべき要件】** 〇調達方法・方式の策定支援 ・案件の規模や性質を踏まえ、最適な調達方式を検討し、提案すること。 〇調達仕様書（案）、応札資料作成要領（案）、評価手順書、評価項目一覧等の調達手続きに係わる資料の作成支援 ・要件定義書を基に、設計・開発業者を調達するための調達仕様書（案）及び応札資料作成要領（案）を作成すること。なお、調達仕様書（案）の作成においては、特定の技術や機器・ツールを前提とすることなく、公正・中立な観点から作成すること。 ・調達方式に合わせて、業者選定に必要となる資料（評価手順書・

項目	内容
	評価項目一覧・適合証明書等）を作成すること。 〇意見招請への対応支援 ・意見招請を実施する場合は、意見招請で寄せられた意見や質問に対する回答案の作成を支援すること。 ・意見招請の結果を踏まえ、必要に応じて調達仕様書（案）を修正し、最終化を行うこと。 〇応札事業者の評価支援 ・技術審査を支援し、評価結果を当省に報告すること。なお、応札業者から提出された提案書及び適合証明書等のすべての項目に対して、調達仕様書の要件を満たしているかどうかを検討し、不明瞭な記載又は要件を満たしていない箇所を一覧表にまとめ、提出すること。 **【2.案件の種類・特性によって追記すべき要件】** ●特定情報システムに該当する場合 〇調達計画書（案）の作成支援 「情報システムに関わる政府調達の基本指針」を踏まえて、調達計画書（案）を作成すること。 〇政府全体管理組織及び府省全体管理組織の指摘事項対応支援 作成した成果物に対して政府全体管理組織・府省全体管理組織から質問や指摘があった場合は、資料作成や説明の支援を行うこと。
案件・情報システムの特性等による留意点	「情報システムに係る政府調達の基本指針」において、特定情報システム（設計・開発の予定価格が 5 億円を超えるもの）に関しては調達計画書の作成は必須となる。
セキュリティに関する留意点	―

6.2.2.3.納入成果物と提出のタイミング

納入成果物とタイミングをまとめると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。

役務内容	納入成果物	納入期限
1. 最適化計画の確認・評価・改善・効果算定	最適化計画の確認・評価・改善・効果算定に関する報告書	契約締結後 （半年の案件の場合の例： 契約締結後 1 ヶ月半程度後）
2. 要件定義の支援	要件定義書	契約締結後 （半年の案件の場合の例： 契約締結後 2 ヶ月半程度後）
3. システムコストの試算	システム構築経費積算書 運用経費積算書	要件定義実施後
4. 調達業務の支援	調達計画書（案） 調達仕様書（案） 応札資料作成要領（案） 評価手順書（案） 評価項目一覧（案） 評価基準書（案） 評価採点表（案） 意見招請回答管理表 入札公示に係わる説明資料（案） 入札公示後に必要となる予算根拠となる説明資料（案）	府省庁の定める時期

6.2.2.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	インプット	インプットを提示するタイミング
1. 最適化計画の確認・評価・改善・効果算定	最適化計画	最適化計画の策定時点
2. 要件定義の支援	システム化計画書 最適化計画 （1 を反映したもの）	仕様書リリース時点 府省庁の定める時期
3. システムコストの試算	要件定義書 （2 の成果物）	要件定義作業後
4. 調達業務の支援	最適化計画 要件定義書 （2 の成果物）	要件定義作業後

（※平成 22 年　次期〇〇省基盤情報システム要求仕様書作成等支援業務　一式）

	平成 22 年度								
	7月	8月	9月	10月	11月	12月	1月	2月	3月
最適化計画の確認・評価・改善提案及び最適化効果の試算				→	→				
次期システム調達計画書案の作成				→	→				
意見招請向け仕様書の作成等	（素案作成）			→	→	→			
			（最終案作成）				→	→	→
意見招請向け仕様書（要件定義書）案に基づくシステム経費の試算			（案作成）		→	→			
			（積算書作成）				→	→	→
技術審査等支援にかかる WBS 項目案の作成等						→	→		

（参考）

最適化計画改定　（案作成）	→	→	→	→	→				
（省内調整・承認手続）					→	→			
次期システム要求仕様　（仕様書作成）	→	→	→	→	→	→	→		
（省内・総務省との調整）								→	→

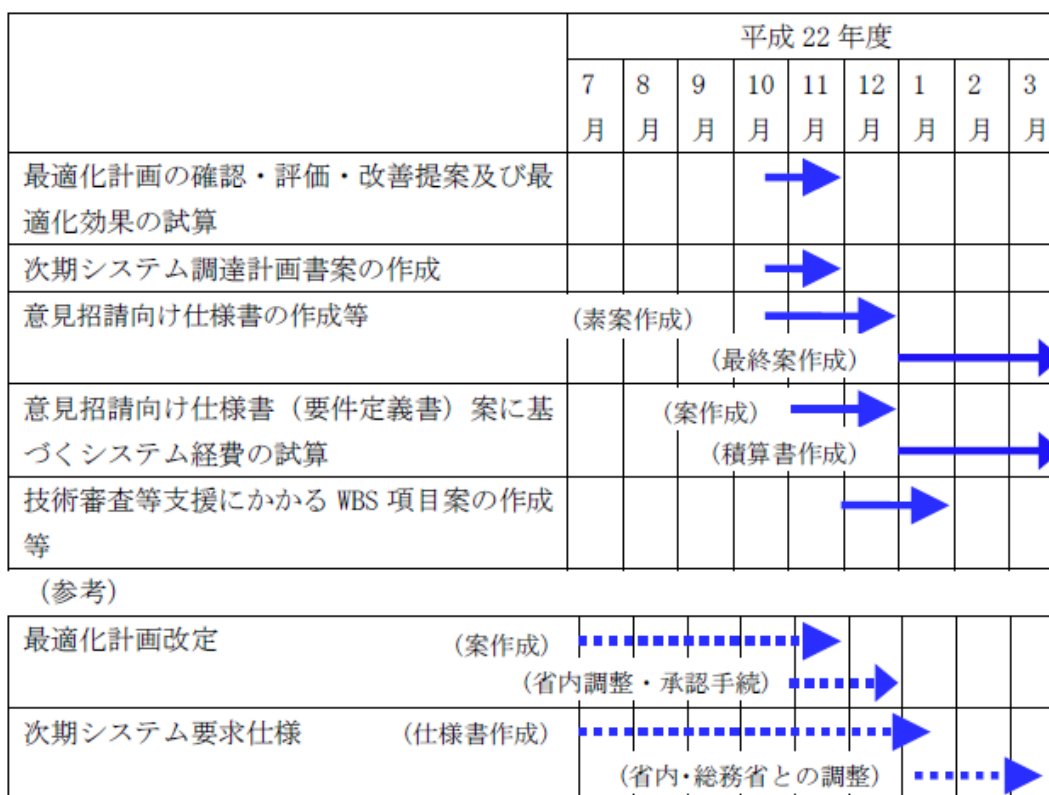



図 6.2-3 全体スケジュール表の例

6.2.3.プロジェクト管理など設計・開発以降における調達支援

6.2.3.1.調達分野の定義

本項で指す、「プロジェクト管理など設計･開発以降における調達支援」は設計･開発工程以降におけるプロジェクト管理等の調達支援等の支援業務を指す（図 6.2-1 及び図 6.2-4 参照)。

図 6. 2-4 情報システムの工程における本役務の範囲

6.2.3.2.仕様書に記載すべき役務内容

6.2.3.2.1.代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [5]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[6]の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

<table>
<tr><th>役務作業</th><th>役務作業の概要</th><th>共通フレーム 2007 のアクティビティ</th><th>調達基本指針に対応する仕様書の章・節（及びそのタイトル）</th></tr>
<tr><td>1. プロジェクト管理</td><td>プロジェクト計画策定、進捗管理、課題管理、変更管理、品質管理、リスク管理</td><td rowspan="3">1.2.4 計画立案
1.2.5 実行及び管理</td><td rowspan="3">—</td></tr>
<tr><td>2. 調達支援</td><td>調達計画書の作成、調達仕様書の作成、意見招請対応、事業者の評価等、調達関連業務の支援</td></tr>
<tr><td>3. その他作業支援</td><td>成果物の管理、会議体の運営</td></tr>
</table>

---

[5] 独立行政法人 情報処理推進機構 共通フレーム 2007
ソフトウェアライフサイクルプロセス SLCP-JCF 2007

[6] 総務省 情報システムに関わる政府調達の基本指針 2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

6.2.3.2.2.各役務内容に関する説明及び仕様書上の記載例

1．プロジェクト管理

項目	内容
役務作業内容の概要	プロジェクト計画を策定し、プロジェクト管理方法等を定義する。 進捗管理、課題管理、変更管理、品質管理、リスク管理といった各種管理を実施する。
想定されるインプット （発注者側で用意）	・システム化構想書 ・システム化計画書 ・最適化計画 ・要件定義書
成果物 （受注者側で用意）	・プロジェクト管理計画書 ・プロジェクト管理報告書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要件】** ・プロジェクト計画策定 ・進捗管理 ・課題管理 ・変更管理 ・品質管理 ・リスク管理 **【2.案件の種類・特性によって追記すべき要件】** ・EVMによる進捗管理
仕様書記載上の例/説明	**【1.基本的に記載すべき要件】** ○プロジェクト計画策定 プロジェクト管理作業の推進方法、管理に用いる指標等を定めた、プロジェクト計画を策定すること。 このとき、プロジェクト計画において、プロジェクト関係者の役割、関係者間の連絡方法、会議体等についても明確にすること。 ○進捗管理 進捗管理に必要となる、WBSやその他必要となる資料の提出をシステム開発業者に指示すること。なお、当該資料の満たすべき要件を業者に提示すること。 システム開発業者の作業状況を定期的に確認し、当初のスケジュールから遅延が発生している場合は、原因・影響等を把握した上で、遅延回復に向けた対応策の検討支援を行うこと。 ○課題管理 プロジェクトの進行に影響を及ぼす課題について管理を行い、課題

	解決に向けた役割分担の検討、解決期限の管理及び解決策の検討支援等を行うこと。 ○変更管理 システムの仕様変更に当たり、各仕様変更案件の重要度・対象・実施時期等に関する検討状況を管理すること。 ○品質管理 システム開発業者の成果物及び提示した資料について内容を確認し、不備等があった場合には質問又は指摘をすることで成果物等の品質の向上を図ること。 ○リスク管理 プロジェクトの進行に影響を及ぼす可能性のあるリスクを抽出し、リスク軽減や回避等、解決に向けた対応策を提示すること。 **【2.案件の種類・特性によって追記すべき要件】** ●最適化対象のシステムの場合 ○EVM による進捗管理 システム開発の作業における発注者及び受注者で協議・合意された WBS を基に、EVM（Earned Value Management）による定量的な進捗管理及び報告を行うこと。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	－

2. 調達支援

項目	内容
役務作業内容の概要	調達計画書の作成、調達仕様書の作成、意見招請対応、事業者の評価等、設計・開発の調達に係わる業務の支援を行う。
想定されるインプット （発注者側で用意）	・最適化計画（※存在する場合のみ） ・要件定義書
成果物 （受注者側で用意）	・調達計画書（案） ・調達仕様書（案） ・応札資料作成要領（案） ・評価手順書（案） ・評価項目一覧（案） ・評価基準書（案） ・評価採点表（案） ・意見招請回答管理表 ・入札公示に係わる説明資料（案） ・入札公示後に必要となる予算根拠となる説明資料（案）
仕様書に記載すべきポイント	**【1.基本的に記載すべき要件】** ・調達方法・方式の策定支援 ・調達仕様書（案）、応札資料作成要領（案）、評価手順書、評価項目一覧等の調達手続きに係わる資料の作成 ・意見招請への対応支援 ・応札事業者の評価支援 **【2.案件の種類・特性によって追記すべき要件】** （特定情報システムに当たる案件） ・調達計画書（案）作成 ・政府全体管理組織及び府省全体管理組織の指摘事項対応支援
仕様書記載上の例/説明	**【1.基本的に記載すべき要件】** ○調達方法・方式の策定支援 ・案件の規模や性質を踏まえ、最適な調達方式を検討し、提案すること。 ○調達仕様書（案）、応札資料作成要領（案）、評価手順書、評価項目一覧等の調達手続きに係わる資料の作成 ・要件定義書を基に、設計・開発業者を調達するための調達仕様書（案）及び応札資料作成要領（案）の作成を実施すること。なお、調達仕様書（案）の作成においては、特定の技術や機器・ツールを前提とすることなく、公正・中立な観点から作成すること。 ・調達方式に合わせて、業者選定に必要となる資料（評価手順書・評価項目一覧・適合証明書等）を作成すること。

項目	内容
	○意見招請への対応支援 ・意見招請を実施する場合は、意見招請で寄せられた意見や質問に対する回答案の作成を支援すること。 ・意見招請の結果を踏まえ、必要に応じて調達仕様書（案）を修正し、最終化を行うこと。 ○応札事業者の評価支援 ・技術審査の支援を実施し、評価結果を当省に報告すること。なお、応札業者から提出された提案書及び適合証明書等のすべての項目に対して、調達仕様書の要件を満たしているかどうかを検討し、不明瞭な記載又は要件を満たしていない箇所を一覧表にまとめ、提出すること。 **【2.案件の種類・特性によって追記すべき要件】** ●特定情報システムに該当する場合 ○調達計画書（案）の作成 指針等及び「情報システムに関わる政府調達の基本指針」を踏まえて、調達計画書（案）を作成すること。 ○政府全体管理組織及び府省全体管理組織の指摘事項対応支援 作成した成果物に対して政府全体管理組織・府省全体管理組織から質問や指摘があった場合は、資料作成や説明の支援を行うこと。
案件・情報システムの特性等による留意点	情報システムに係る政府調達の基本指針において、特定情報システム（設計・開発の予定価格が 5 億円を超えるもの）に関しては調達計画書の作成は必須となる。
セキュリティに関する留意点	―

3. その他作業支援

項目	内容
役務作業内容の概要	成果物の管理、会議体の運営等、発注者側が行う作業の支援を行う。
想定されるインプット （発注者側で用意）	―
成果物 （受注者側で用意）	・成果物管理計画書（案）（※） ・コミュニケーション管理計画書（案）（※） ・議事録（案） （※）プロジェクト管理計画書で定義されている場合は別途用意する必要はない。
仕様書に記載すべきポイント	**【1.基本的に記載すべき要件】** ・成果物の管理 ・会議体の運営
仕様書記載上の例/説明	**【1.基本的に記載すべき要件】** 〇成果物の管理 ・システム開発業者が納品すべき成果物について不足がないか、品質上問題ないかを確認し、発注者が検収を行う支援を行うこと。 ・納品された成果物のバージョン管理を支援すること。 〇会議体の運営 ・プロジェクトにおける会議体を定義し、出席者・運営主体等を明確にする支援を行うこと。 ・本業務の受注者が運営主体となる会議について、会議開催後〇営業日以内に議事録（案）を作成し提示すること。 ・発注者が運営主体となる会議について、必要に応じて会議資料の作成を支援すること。
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	―

6.2.3.3.納入成果物と提出のタイミング

納入成果物とタイミングをまとめると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。

役務内容	納入成果物	納入期限
1. プロジェクト管理	プロジェクト計画書 プロジェクト管理報告書	プロジェクト計画書は契約締結後１カ月以内 プロジェクト管理報告書は月次
2. 調達支援	調達計画書（案） 調達仕様書（案） 応札資料作成要領（案） 評価手順書（案） 評価項目一覧（案） 評価基準書（案） 評価採点表（案） 意見招請回答管理表 入札公示に係わる説明資料（案） 入札公示後に必要となる予算根拠となる説明資料（案）	府省庁の定める時期
3. その他作業支援	議事録	会議開催後○営業日以内

6.2.3.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	インプット	インプットを提示するタイミング
1. プロジェクト管理	―	―
2. 調達支援	最適化計画 要件定義書	要件定義作業後
3. その他作業支援	―	―

6.2.3.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表を作成することが必要である。

6.3.システム構築（設計・開発）

本章では、情報システムの設計、開発、移行、運用設計などの情報システムの構築に係わる役務作業について取り扱う。

図 6.3-1 役務調達の分類における対応箇所

6.3.1.調達分野の定義

システム構築（設計・開発）における役務は、情報システムを構築する状況から新規開発、システム更改、ハードウェア更改、機能追加の 4 通りに定義した。

下記にそれぞれの役務の定義を記載する。

役務	定義
新規開発	これまで情報システムが存在しなかった業務を対象として、新たに情報システムを開発するシステム開発案件を指す。
システム更改	法律の変更、業務の変更などに伴うアプリケーションの全面更改、システム統合などのシステム開発案件を指す。
ハードウェア更改	ハードウェアの更改に伴うアプリケーションのマイグレーション（移植）のためのシステム開発案件を指す。

機能追加	サブシステムレベルの機能追加案件、既存システムの設計、開発事業者・保守事業者が契約範囲内で対応する範囲を超えたシステム改修案件を指す。 サブシステムレベルより小規模な追加については、「6.6.3 アプリケーション保守」を参照のこと。

6.3.2 仕様書に記載すべき役務内容

6.3.2.1.代表的な役務作業の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [7]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[8]の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務作業の概要	共通フレーム 2007 の アクティビティ	調達基本指針に対応する仕様書の章・節
1. 開発環境の準備	開発に必要な機材（ハードウェア、開発ツール等）、作業場所などの確保	1.6.1 プロセス開始の準備	2 章(5.1)　作業内容 12 章(2)　開発方法
2. 開発実施計画の作成	設計・開発実施計画（スケジュール、体制、役割分担、作業内容、開発環境、開発方法、開発ツール、成果物など）の作成	1.6.1 プロセス開始の準備	2 章(5.1)　作業内容 12 章(2)　開発方法
3. 基本設計	要件定義に基づく、機能設計（業務機能等）、データ設計（概念モデル・論理モデル）、画面設計、帳票設計、システム方式設計、外部インタフェース設計、情報セキュリティ設計 ※機能追加は、上記の一部のみ	1.6.2 システム要件定義 1.6.3 システム方式設計 1.6.4 ソフトウェア要件定義 1.6.5 ソフトウェア方式設計	2 章(5.1)　作業内容 12 章(2)　開発方法
4. 詳細設計	基本設計に基づく、・プログラム設計（開発するプログラム一覧及び仕様定義等）、データ設計（物理モデル）、画面設計、帳票設計、システム方式設計、外部インタフェース設計、情報セキュリティ設計	1.6.6 ソフトウェア詳細設計	2 章(5.1)　作業内容 12 章(2)　開発方法

7 独立行政法人　情報処理推進機構　共通フレーム 2007
ソフトウェアライフサイクルプロセス　SLCP-JCF 2007
8 総務省　情報システムに関わる政府調達の基本指針　2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

役務作業	役務作業の概要	共通フレーム2007の アクティビティ	調達基本指針に対応する仕様書の章･節
5.単体テスト･結合テスト･総合テスト･他システム接続テスト	詳細設計に基づく、ソースコードの作成 テスト実施計画書の作成と担当課の承認の受領 テストに必要な機器･ツールの準備 各テストを実施し、発見された不具合への対応 テスト結果報告書の作成	1.6.7 ソフトウェアコード作成及びテスト 1.6.8 ソフトウェア結合 1.6.9 ソフトウェア適格性確認テスト 1.6.10 システム結合 1.6.11 システム適格性確認テスト	2章(5.1)　作業内容 8章　テスト要件定義 12章(2)　開発方法
6.受入テスト支援	受入テスト手順書案の作成や、不具合発生時の調査及び対策実施、運用テストの実施など、発注者が実施する受入テストの支援	1.6.13 ソフトウェア受入れ支援	2章(5.1)　作業内容 12章(2)　開発方法
7.移行	業務に必要となるデータの移行作業や初期データの投入 開発環境から本番環境への移行作業	1.8.5移行	2章(5.1)　作業内容 9章(1)　移行に係る要件 12章(2)　開発方法
8.利用者教育	教育訓練実施計画および、システム利用マニュアルの作成 府省職員向け研修の実施	1.6.13 ソフトウェア受入れ支援	2章(5.1)　作業内容 9章(2)　教育に係る要件
9.運用･保守事業者への引継ぎ	運用設計 運用事業者･保守事業者への引継ぎ	1.7.1 プロセス開始の準備 1.8.1 プロセス開始の準備	2章(5)　作業内容･納入成果物
10.プロジェクト管理	進捗管理、文書管理、情報セキュリティ管理、課題･問題管理、変更管理、構成管理など設計･開発業務のプロジェクト管理を実施	3.1.2 計画立案 3.1.4 実行及び管理	2章(5.1)　作業内容 12章(2)　開発方法
11.検収	必要な納入成果物の納入を行い、修正が必要と判断された場合には改修	1.2.7 納品および完了	2章(5)　作業内容･納入成果物

6.3.2.2.各役務内容に関する説明及び仕様書上の記載例

前節で述べた役務作業の内容の多くは、新規開発、システム更改、ハードウェア更改、機能追加の役務パターンによらず共通である。したがって、本節の説明では、とくに断らない限り共通な事項であり、必要に応じてどの役務パターンであるかを示すものとする。

1. 開発環境の準備

項目	内容
役務内容の概要	開発に必要な機材、作業場所などの確保
想定されるインプット （発注者側で用意）	・ 新システムインフラの概要（予定） ・ 動作環境 ・ 運用条件 ・ 要件定義書
成果物 （受注者側で用意）	－
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ システム設計・開発に必要な環境（作業場所、機器、備品消耗品）の構築 ・ 開発環境の管理
仕様書記載上の例/説明	**仕様書に記載する場合の例** ・ システム設計・開発に必要な開発用機器は、請負事業者が準備し負担すること。 ・ 開発に係わる環境（機器、作業室等）に対して充分なセキュリティ対策を実施すること。
案件・情報システムの特性等による留意点	オンサイトでの開発環境が準備できない場合は、開発リポジトリの構築も行うことも検討の余地がある。
セキュリティに関する留意点	開発環境のセキュリティ対策 ・ 開発に係わる環境（機器、作業室等）を受注者側が用意する場合には、これらの環境に対しても充分な情報セキュリティ対策を実施すること

2. 開発実施計画の作成

項目	内容
役務内容の概要	設計・開発実施計画の作成
想定されるインプット （発注者側で用意）	・ 要件定義書 ・ 主要業務概要一覧 ・ 受託者と関連業者の関係 ・ 関連業者の作業概要 ・ 業務スケジュール ・ 役割分担表 ・ 府省庁のドキュメント標準
成果物 （受注者側で用意）	・ プロジェクト計画書 ・ 設計・開発実施計画書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 設計・開発実施計画について、最適化指針等政府の統一基準に沿って受託事業者が案を作成し、府省と調整の上、最終化 ・ プロジェクト計画を策定し、WBS（Work Breakdown Structure）、クリティカルパス、マイルストーンを明示したプロジェクト計画書を作成すること。 **【2.必要に応じて記載すべき要求要件】** ・ 標準記述様式や標準規約等の定義と、それに基づいて開発が行われていることのレビューを実施すること。
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○プロジェクト計画 受託者は、プロジェクト計画を策定すること。プロジェクト計画の策定においては、以下に示す作業を実施すること。 ・ プロジェクト計画の策定前に、本システムの本稼動までに必要な作業を整理し、WBS を作成すること。また、タスク毎に作業内容、納入成果物、開始条件及び終了条件を明確にすること。なお、タスクの詳細化は各工程開始前に実施し、具体的な進捗状況及び投入実績値を把握できる単位にまで可能な限り詳細化すること。 ・ 各タスクの従属関係とクリティカルパス（プロジェクトの完成を遅らせないために、遅らせることができないタスクの集まり）を明確にし、タスク毎に開始日、完了日及び中間マイルストーンを決定すること。 ○設計・開発実施計画 ・ システム化にあたっての基本的な方針について、成果物と関連付けた作業スケジュール、作業内容、作業担当者、レビュー実施計

	画、チェックポイント、開始条件・終了条件等、プロジェクトの作業工程を定義するドキュメント等を「プロジェクト計画書」に取りまとめ、その内容について本省と協議のうえ、承認を得るとともに、当該「プロジェクト計画書」に基づき、実際の設計・開発業務を実施すること。 ○スケジュール ・　全体スケジュールと主要マイルストーンを設定したスケジュールを記述する。 ○プロジェクト体制 ・　各組織のリーダー、担当者、連絡方法等、プロジェクト参加者にとって必要となる情報を記述する。 ・　プロジェクト全体の管理責任の帰属および管理内容について明確化する。 ○役割分担 ・　全事業者の役割分担を明らかにし、各事業者がプロジェクト全体における自らの役割を認識できるようにする。
案件・情報システムの特性等による留意点	府省によってはドキュメントを分けて提出を求める場合も存在する。こうした点に関しては各府省で定められている調達方針・ガイドラインに沿う事が望ましい。 追加案件や改修案件が発生する可能性を考慮する場合は、見積書等の作成や必要工数の算出といった作業が発生する場合がある旨も仕様書に記述する必要がある。 作業およびスケジュールは、外部報告用のものと内部管理用のものを 2 種類用意することもある。その際は、外部報告用のものは外部関係者が理解しやすい表現としたものを作成し、内部管理用のものは WBS に進捗状況を付加したものなどを作成し管理することが望ましい。 受託事業者の作業だけでなく、担当府省を始めとする受託事業者外担当者の作業も計画の中で定義することが望ましい。受託事業者外担当者の作業を定義する際は、調整が必要となるため、素案を作成した時点で担当府省に相談する。
セキュリティに関する留意点	－

3. 基本設計

項目	内容
役務内容の概要	要件定義に基づく、機能設計、データ設計、画面設計、帳票設計、システム方式設計、外部インタフェース設計、情報セキュリティ設計
想定されるインプット （発注者側で用意）	・ 要件定義書 ・ 現行システムの基本設計書（新規開発を除く） ・ 各府省で定めるセキュリティポリシー ・ 政府機関の情報セキュリティ対策のための統一基準
成果物 （受注者側で用意）	・ 基本設計書 （機能設計書、データ設計書、画面設計書、帳票設計書、システム方式設計書、外部インタフェース設計書が分冊化されることがある）
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 基本設計書作成項目 ・ 設計環境、作業場所を受託者の負担と責任で準備 ・ 法律改正により設計に変更が生じた場合の対応 ・ 調達システムの関連事業者との連携 ・ テスト環境や保守環境の設計 **【2.必要に応じて記載すべき要求要件】** ・ 汎用パッケージを中心とした設計を前提とする場合は、業務要件のプロセスと導入するパッケージの適合具合とずれ具合の分析（機能追加を除く）
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○基本設計書作成項目 ・ 機能設計（業務機能、例外処理設計及び運用機能等の設計） ・ データ設計（E-R 図等を用いた概念モデル及び論理モデルの設計） ・ 画面設計 ・ 帳票設計 ・ システム方式設計（ソフトウェア構成及びハードウェア構成等の技術基盤の設計） ・ 外部インタフェース設計 ・ 情報セキュリティ設計 ○設計業務共通要件 ・ 本システムが稼動する本番環境のほか、テスト環境及び保守環境の設計を行うこと。 ・ 設計環境（設計用のハードウェア、ミドルウェア及び設計ツール

	等)、作業場所等は、受託者の負担と責任において準備すること。 ・プロジェクト計画書に定める構成・変更管理要領に基づいて管理すること。 ・別途調達予定の工程管理業者、本システム関連業者及び他システムに係る業者等と連携して作業すること。 〇汎用パッケージを中心とした設計 ・本システムは、汎用パッケージソフトウェアの利用を前提とした開発となるため、基本設計工程においては、本書が求める業務要件のプロセスと導入する汎用パッケージソフトウェアが、どれだけ適合（フィット）し、ずれ（ギャップ）が生じるのか、フィット・ギャップを分析すること。
案件・情報システムの特性等による留意点	案件によっては、１つの調達事業者が要件定義と設計・開発の両方を行うことになるが、要件定義に関する記載ポイントは、「6.2.1 要件定義」を参照
セキュリティに関する留意点	情報セキュリティ設計 ・「政府機関の情報セキュリティ対策のための統一基準」、及び各府省の情報セキュリティポリシーに準拠して情報セキュリティ設計を行うこと

4. 詳細設計

項目	内容
役務内容の概要	基本設計に基づく、プログラム設計、データ設計、画面設計、帳票設計、システム方式設計、外部インタフェース設計、情報セキュリティ設計
想定されるインプット （発注者側で用意）	・ 現行システムの詳細設計書、プログラムソース（新規開発を除く）
成果物 （受注者側で用意）	・ 詳細設計書 （プログラム設計書、データ詳細設計書、画面詳細設計書、帳票詳細設計書、システム方式詳細設計書、外部インタフェース詳細設計書が分冊化されることが多い）
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 詳細設計のアウトプット項目 **【2.必要に応じて記載すべき要求要件】** ・ 関連事業者に対する協力
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○詳細設計のアウトプット項目 ・ プログラム設計（開発するプログラム一覧、仕様定義等） ・ データ設計（物理モデル） ・ 画面・帳票設計（使用する開発ツールを基にした設計） ・ システム方式設計（使用するソフトウェア・ハードウェアを基にした設計） ・ 情報セキュリティ設計（使用するソフトウェア・ハードウェアを基にした設計） ○関連事業者 ・ 関連する事業者に対して必要に応じて設計資料を提示するとともに、問合せに対する回答等を実施すること。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	情報セキュリティ設計 ・ 「政府機関の情報セキュリティ対策のための統一基準」、及び各府省の情報セキュリティポリシーに準拠して情報セキュリティ設計を行うこと

5．単体テスト・結合テスト・総合テスト・他システム接続テスト

項目	内容
役務内容の概要	詳細設計に基づく、ソースコードの作成 テスト実施計画書の作成と担当課の承認の受領 テストに必要な機器・ツールの準備 各テストを実施し、発見された不具合への対応 テスト結果報告書の作成
想定されるインプット （発注者側で用意）	－
成果物 （受注者側で用意）	単体テスト、結合テスト、総合テストに関わる以下のデータおよび文書 ・テストデータ ・テスト実施計画書 ・テスト実施要領（テスト仕様書） ・テスト結果／品質評価報告書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・テスト実施計画書作成 ・テスト実施要領作成 ・テストデータ作成 ・単体テスト、結合テスト、総合テストの概要 ・不良修正の扱い、原因の究明 ・テスト結果／品質評価報告書作成
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○テスト実施計画書作成 　実施する単体テスト、結合テスト、総合テストについて、テスト方針、実施内容及び実施理由を記載し、テスト工程毎にテスト実施計画書として提出すること。 　　テスト実施計画書に記載すべき事項を以下に示す。 （1）　受託者のテスト実施体制と役割 （2）　テストに係る詳細な作業及びスケジュール （3）　テスト環境（テストにおける回線及び機器構成、テスト範囲） （4）　テストツール （5）　テストデータ （6）　評価指標 ○テスト実施要領作成 各テストを行うため一連のテストケース（入力、出力及びテスト基

	準)、テストシナリオ、テストデータ及びテスト手順を整理し、テスト実施要領として準備すること。 ○テストデータ作成 (ア)テストデータは、原則として受託者において用意すること。 (イ)テスト工程毎のテスト計画書にテストデータの種類等を記載すること。 ○単体テスト、結合テスト、総合テストの概要 (1)　単体テスト 開発したモジュール等の単位で、プログラムが正常に動作すること等のテストを行うこと。 (2)　結合テスト プログラム及びモジュールが、本システム全体において、正しく機能することを確認するため、段階的に結合した状態でテストを行い、ソフトウェアの結合が完全であることを確認すること。 (3)　総合テスト (ア)本システムが要求どおりに構築されていることを確認可能なテストを行うこと。 (イ)本システムが納入可能であることを確認すること。 (ウ)ソフトウェアが仕様に適合し、かつ本番環境で利用可能であることを確認できる評価指標を設定した上で、テストを実施すること。 (エ)性能及び負荷のテストにおいては、本番環境と同様の環境により負荷等をかけ、問題が発生しないことを確認すること。 (オ)以下の項目について確認を行うこと。 ①　機能性 ・　システム機能が、正常系、異常系ともに仕様書どおりに動作すること。 ・　他システムとの業務連携処理が正常に機能すること。 ・　情報セキュリティ要件を満たしていること。 ②　信頼性 ・　信頼性要件を満たしていること。 ・　障害が発生した際の回復処理が適切であること。 ③　操作性 ・　要件及び説明書どおりに動作し、利用者が利用しや

	すいこと。 ④　性能性 ・　オンライン処理、バッチ処理の応答時間、スループットが適切であること。 ・　システムの限界条件（データ量、処理量）下で、正常に動作すること。 ○不良修正の扱い、原因の究明 ・　不良を修正した場合、当該修正によって他プログラムに負の影響がないことを確認 不良の原因について、プログラミングミス、設計不良のほか、担当者についても調査・分析（例えば、特定の担当者が設計・開発を行ったモジュール、コンポーネントに不良が集中する場合、同担当者が設計・開発した他モジュール、コンポーネントについて、不良がないことを重点的に検査する等。） ○テスト結果／品質評価報告書 プログラム規模に対するテストケース数、不良検出件数の合計、プログラム規模に対する不良検出率、テスト完了件数／テスト計画件数、実績不良件数／予測不良件数などを報告
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	テスト環境のセキュリティ対策 ・テスト環境（機器、作業室、テストデータ等）を受注者が用意する場合は、これらの環境に対しては充分なセキュリティ対策を実施すること

6. 受入テスト支援

項目	内容
役務内容の概要	受入テスト手順書案の作成や、不具合発生時の調査及び対策実施、運用テストの実施など、発注者が実施する受入テストの支援
想定されるインプット（発注者側で用意）	—
成果物（受注者側で用意）	・受入テスト手順書案 ・受入テスト実施報告書案
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・受入テスト手順書案の作成 ・受入テストサポート要員の確保 ・受入テスト環境の構築 ・受入テストデータの準備 ・障害の解析および対応策の提示 ・府省が作成する対応案に沿ったプログラム修正の実施
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇受入テスト手順書案の作成 ・ 受入テスト実施者が行う具体的な手順及び結果を記入するための受入テスト手順書案を作成すること。システム操作に精通していない職員でも分かりやすいテストとなるように工夫すること。 〇受入テストサポート要員の確保 ・ 受入テストは当省が主体となって行うが、求めに応じて受入テストをサポートするための要員を確保すること 〇受入テスト環境の構築 ・ 可能な限り本番環境と同等の受入テスト実施環境を準備すること。 〇受入テストデータの準備 ・ 受入テストで必要となるテストデータについて準備すること 〇障害の解析および対応策の提示 ・ 受入テストで確認された障害について解析を行い，対応方針を当省の承認を得ること。 〇府省が作成する対応案に沿ったプログラム修正の実施 ・ 承認を得た対応方針に基づいて修正する。
案件・情報システムの特性等による留意点	多拠点でのシステム導入を行う大規模案件の場合は、一部拠点において受入テストを先行的に実施することが望ましい
セキュリティに関する留意点	—

7. 移行

項目	内容
役務内容の概要	移行作業に係る各種計画書および手順書の作成 本番環境でのシステム移行リハーサルおよび本番移行
想定されるインプット （発注者側で用意）	・ 投入対象データ ・ 移行導入業務のイメージ図
成果物 （受注者側で用意）	・ 移行実施計画書 ・ 移行実施手順書 ・ 移行リハーサル仕様書 ・ 移行リハーサル結果／品質評価報告書 ・ 移行プログラム ・ 移行データ ・ 移行結果報告書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** 新規開発 ・ 発注者が行う移行データの仕様決定および調整作業の支援 ・ 必要に応じて移行ツールやプログラムを作成 ・ 紙媒体からのデータエントリーおよび既存システムからのデータ抽出・移行作業 以下、新規開発では開発環境から本番環境への移行があるときのみ記載。新規開発以外は必須。 ・ 移行実施計画書を作成 ・ 移行実施手順書を作成 ・ 移行リハーサル仕様書を作成 ・ 本番環境において移行リハーサルを実施 ・ 移行リハーサル結果／品質評価報告書を作成 ・ 本番移行作業を実施 ・ 移行結果報告書を作成
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇新規開発 ・ 調達事業者は、移行対象データの内容や形式を事前に確認して、移行方法（空白やデータがない項目やデータ型の違いなどの対処）について、〇〇省の担当者と確認して移行作業を実施すること。移行に際しては、必要に応じて移行ツールやプログラムを作成して実施すること。 ・ 本システムの利用に必要なマスタデータの作成及び登録並びに

	過去の業務データの変換及び導入を移行業務の対象とし、移行に必要な作業分担を関連する府省の役割を含めて明確にし、移行作業体制を整備すること。移行作業に当たっては、次に示す手順で作業を実施すること。 ① 移行の対象となるデータを主管課と相談の上整理する。 ② 本システムに移行するためのデータ形式を定め、必要に応じてその形式から本システムに取り込むためのツールを作成する。 ③ データ形式に合わせて新規にデータを入力し、又は既存のデータを変換して移行データを作成する。 ④ 移行ツール等を使用してデータを本システム内に取り込む。 ⑤ 移行後のデータが正しく取り込まれているか検証する。 ⑥ エラーデータを修正し、正しく修正されていることを再度確認する。 〇移行 ・ 請負者は、既存データを受領することを前提に、必要に応じ、本システムデータベースへの移行プログラムの設計・開発、移行作業、移行後のデータに関する正当性確認等、移行にあたって必要となる各種作業を実施すること。 ・ 移行計画書に従い、導入済み本番環境に対してデータの移行を実施する。データ移行実施時は、移行計画書に従って事前にリハーサルを実施すること。 **説明** ・ 移行実施計画書 移行実施体制と役割、移行に係る詳細なスケジュール、移行環境、移行方法、移行ツール準備方法などを記載 ・ 移行実施手順書 本番移行における作業内容、確認方法、判定基準、問題発生時の対応内容（コンテンジェンシープラン)、タイムスケジュールなどを記載 ・ 移行リハーサル仕様書 移行リハーサルにおける作業内容、確認方法、判定基準、問題発生時の対応内容、タイムスケジュールなどを記載
案件・情報システムの特性等による留意点	移行データ抽出仕様の作成は設計・開発事業者が行い、実際のデータ抽出作業は運用事業者が行うケースなど、移行プロセスでは関連事業者との役割分担が生じやすいため、どの事業者が何を担当するかというタスクの明確化が重要である。
セキュリティに関する留意点	―

8. 利用者教育

項目	内容
役務内容の概要	教育訓練実施計画および、操作マニュアルの作成 府省職員向け研修の実施
想定されるインプット （発注者側で用意）	・ 教育研修の対象者、実施場所、実施期間 ・ 操作マニュアル（現行）　（新規開発以外）
成果物 （受注者側で用意）	・ 教育実施計画書 ・ 研修用テキスト ・ 操作マニュアル
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 操作マニュアルの作成 ・ システム利用者向け研修の開催要件（規模や期間） **【2.必要に応じて記載すべき要求要件】** 利用拠点数や利用者数が大規模となるシステムにおいては、下記のような作業を通じて、効率的な教育環境の調達を行うことが望ましい。 ・ 教育実施計画書の作成 ・ e ラーニング機能の提供
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○操作マニュアルの作成 ・ 機器の操作方法及び本システム利用方法を記載した、操作マニュアルを作成すること。 ○システム利用者向け研修の開催要件（規模や期間） ・ システム利用者向けに、本システムの集合研修を実施すること。また、自己学習のための教材を作成すると共に、教育研修方法及び教材の利用方法等を研修手引書としてとりまとめること ・ ○○省と協議の上、研修用テキストを作成すること。研修用テキストの作成に当たっては、利用者が本システムの操作方法を短期間で習得しやすいように説明方法及び文章を工夫すること。また、それらを通読することで十分に理解できる、分かりやすい内容となるよう工夫すること。 ○教育実施計画書の作成 ・ 教育研修内容の立案及び研修計画の策定を行い、教育研修環境、教育研修方法等について記載した教育実施計画書を作成すること。

	・ 伝達研修において、教育研修対象者が本システムの操作方法等を容易に理解できるよう、e-Learning 機能を提供し、必要に応じて中央研修を撮影した教材の配布等の措置を講じること。なお、教材等を配布する場合は、受託者が必要部数用意すること。
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	利用者教育 ・ システム利用者向けに、情報セキュリティに関する教育を行うこと。

9. 運用･保守事業者への引継ぎ

項目	内容
役務内容の概要	運用設計 運用管理事業者・保守事業者への引継ぎ
想定されるインプット （発注者側で用意）	（新規開発以外） ・ 運用設計書（現行システム） ・ 運用マニュアル（現行システム）
成果物 （受注者側で用意）	・ 運用設計書 ・ 運用マニュアル ・ 保守体制表（案） ・ 引継実施計画書 ・ 引継実施報告書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 開発する業務システム及びアプリケーションの運用設計 ・ 運用マニュアルの作成 ・ 引継計画書および引継実施報告書の作成 ・ 新システムの本番稼動前に、運用事業者および保守事業者への引継ぎを実施 ・ 運用マニュアルに関して、運用事業者からの問い合わせや修正依頼が生じた場合、契約期間内において対応
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇運用設計 ・ 開発する業務システム及びアプリケーションの運用設計を行う。運用作業を「業務及びアプリケーションを安全かつ安定的に運用し続けるために必要な作業」とし、体系的かつ網羅的に必要な作業要件を定義し設計すること 〇運用マニュアル ・ 本システムに係る運用業務に必要な運用マニュアルを作成すること。 〇引継計画書 ・ 受託者は、引継ぎ体制・役割、詳細な作業及びスケジュール、引継ぎ方法、引継ぎ結果の評価方法・評価基準等について記述した引継ぎ計画書を作成すること。 また、作成した引継計画書に基づいて引継ぎを実施すること。 引継ぎ実施後、引継実施報告書を作成すること

	○保守業者への引継ぎ ・別途調達予定の○○に係るソフトウェア保守業者による業務は、平成○年度○月より実施することから、受託者は、保守業者の決定後、担当職員と協議し、平成○年○月末までに受託者の負担と責任において、本ソフトウェアの内容等の引継ぎを実施すること。 ○運用業者への引継ぎ ・運用業者が実施する平成○○年度の本稼動後の運用業務の円滑な実施に資するよう、本システムに係る運用業務に必要なドキュメントの整備、作成及び提供を行った上、運用業者に対して訓練期間を設定し、必要な研修訓練等を受託者が実施すること。
案件・情報システムの特性等による留意点	運用向けツールや手順書等が必要な場合は、これを作成し提供すること。
セキュリティに関する留意点	－

10. プロジェクト管理

項目	内容
役務内容の概要	進捗管理、文書管理、情報セキュリティ管理、課題・問題管理、変更管理、構成管理など、設計・開発業務のプロジェクト管理を実施
想定されるインプット （発注者側で用意）	―
成果物 （受注者側で用意）	・ 進捗管理資料 ・ 課題管理表
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 進捗管理 ・ 文書管理 ・ 課題・問題管理 ・ 構成管理 ・ 変更管理 ・ 情報セキュリティ管理
仕様書記載上の例/説明	**説明** ○進捗管理 ・ 進捗管理資料をもとに、進捗状況を定量的に分析し、作業状況を報告する。作業工程毎に会議・情報伝達計画を策定し、定期的なレビューを実施する。計画から遅れが生じている場合は、要員の追加や体制の見直しなどの作業改善策を提示する。 ○文書管理 ・ 受注者は、基本設計結果を修正・更新する際には、〇〇省が作成している「設計・開発段階計画書」の標準管理要領（文書管理要領、変更管理要領、など）にしたがうこと。 ○課題・問題管理 ・ 作業に係る課題を一元管理するとともに、課題の認識、対応案の検討、解決及び報告のプロセスを確立する。 ○構成管理 ・ 本ソフトウェア開発の整合性を維持し、プロジェクト環境の変更に対するトレーサビリティを確保する。 ○変更管理 ・ 調達仕様書及び要件定義書に記載された内容の変更が必要となっ

	た場合、変更の箇所、内容、理由、影響範囲、影響の大きさ等を明確にした上で、早期に担当省庁からの承認を得る。 〇情報セキュリティ管理 ・各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐ。また、発生した場合に被害を最小限に抑える。
案件・情報システムの特性等による留意点	本項では、設計・開発事業者にとってのプロジェクト管理役務について述べている。 情報システム調達全体に係るプロジェクト管理役務に関しては、「6.2.3 プロジェクト管理」を参照すること。 大規模案件の場合は、EVM 進捗管理を行うこと。調達支援業務（工程管理）業者により EVM 管理が実施される場合には、EVM 管理を行う上で進捗管理上報告すべき情報等についても、設計開発事業者の調達仕様書に盛り込んでおく必要がある
セキュリティに関する留意点	情報セキュリティ管理 ・各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと。また、発生した場合には発注への迅速な報告を行った上で被害を最小限に抑えること

11. 検収

項目	内容
役務内容の概要	必要な納入成果物の納入を行い、修正が必要と判断された場合には改修を実施
想定されるインプット（発注者側で用意）	―
成果物（受注者側で用意）	・プロジェクト完了報告書 ・各ドキュメント ・ソースコード、実行モジュール等のプログラム一式
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・プロジェクト完了報告書 ・仕様書において「納入成果物」として示した要件に基づく納入 ・成果物に修正が必要と判断された場合の改修作業
仕様書記載上の例/説明	**仕様書に記載する場合の例** ・本仕様書に示した要件に基づき、納入成果物を納入すること。 ・検査の結果、本省から納入成果物の全部又は一部に修正が必要と判断された場合には、受託者は直に引き取り、必要な改修を行った後、指定した日時までに修正内容を反映したすべての納入成果物を納入すること。
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	―

6.3.3.納入成果物と提出のタイミング

納入成果物とタイミングを記載すると、下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。納入期限は、チェック校正期間を見込んで設定すること。

役務作業	納入成果物	納入期限
1. 開発環境の準備	―	
2. 開発実施計画の作成	プロジェクト計画書 設計･開発実施計画書	受託後 2 週間以内
3. 基本設計	基本設計書	基本設計完了時
4. 詳細設計	詳細設計書	詳細設計完了時
5. 単体テスト･結合テスト･総合テスト･他システム接続テスト	単体テスト、結合テスト、総合テストに関わる以下のデータおよび文書： テストデータ テスト実施計画書 テスト実施要領（テスト仕様書） テスト結果／品質評価報告書	 各テストの開始 2 週間前 各テストの開始 2 週間前 各テストの開始 2 週間前 各テストの終了時
6. 受入テスト支援	受入テスト手順書案 受入テスト実施報告書案	テストの開始 2 週間前 テストの終了時
7. 移行	移行実施計画書 移行実施手順書 移行リハーサル仕様書 移行リハーサル結果/品質評価報告書 移行プログラム 移行データ 移行結果報告書	移行開始前 移行開始前 移行開始前 プロジェクト完了時 プロジェクト完了時 プロジェクト完了時 プロジェクト完了時
8. 利用者教育	教育実施計画書 研修用テキスト 操作マニュアル	プロジェクト完了時
9. 運用･保守事業者への引継ぎ	運用設計書 運用マニュアル 保守体制表（案） 引継実施計画書 引継実施報告書	プロジェクト完了時
10. プロジェクト管理	進捗管理資料 課題管理表	随時 随時
11. 検収	プロジェクト完了報告書 各ドキュメント ソースコード、実行モジュール等のプログラム一式	プロジェクト完了時

6.3.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングは下記の通り。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	インプット	インプットを 提示する タイミング
1. 開発環境の準備	新システムインフラの概要（予定） 動作環境 運用条件 要件定義書	入札公示時に調達仕様書･付属資料に記載する
2. 開発実施計画の作成	要件定義書 主要業務概要一覧 受託者と関連業者の関係 関連業者の作業概要 業務スケジュール 役割分担表 府省内のドキュメント標準	入札公示時に調達仕様書･付属資料に記載する
3. 基本設計	要件定義書 現行システムの基本設計書（新規開発を除く） 各府省で定めるセキュリティガイドライン 政府機関の情報セキュリティ対策のための統一基準	入札公示時に調達仕様書･付属資料に記載する
4. 詳細設計	現行システムの詳細設計書、プログラムソース（新規開発を除く）	詳細設計開始時
5. 単体テスト･結合テスト･総合テスト･他システム接続テスト	—	—
6. 受入テスト支援	—	—
7. 移行	投入対象データ 移行導入業務のイメージ図	入札公示時に調達仕様書･付属資料に記載する
8. 利用者教育	教育研修の対象者、実施場所、実施期間（現行） 操作マニュアル　（新規開発以外）	入札公示時に調達仕様書･付属資料に記載する
9. 運用･保守事業者への引継ぎ	（新規開発以外） 運用設計書（現行システム） 運用マニュアル（現行システム）	入札公示時に調達仕様書･付属資料に記載する
10. プロジェクト管理	—	—
11. 検収	—	—

6.3.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表を作成することが必要である。

新規開発でない場合には、現行の運用事業者・保守事業者等関係する事業者の関わりについて言及が必要である。

以下に示す役割分担表の例は、「情報システムに係る政府調達の基本指針」実務手引書からの引用で、典型的な分離調達プロジェクトにおける主要業務と各事業者の業務上の役割を示している。

役割分担表の例

主要業務	調達担当課室	工程管理 支援事業者	共通基盤 事業者	個別機能 事業者	ハードウェア 等納入事業者	運用事業者	ソフトウェア 保守事業者
プロジェクト管理・推進							
プロジェクト計画書の策定（改訂）							
プロジェクト・スコープの作成	◎	◆	□				
プロジェクト体制の確立	◎	◆	□				
会議体の運営方法作成	◎	◆	□				
スケジュール及び主要マイルストーンの設定	◎	◆	□				
共通 WBS の設定	◎	◆	□				
標準管理要領の作成	◎	◆	□				
プロジェクト標準の作成	◎	◆	□				
プロジェクト推進（プロジェクト管理の実施）							
文書管理	◎□	◆□	○□	□	□	□	□
情報セキュリティ対策要領	◎□	◆□	○□	□	□	□	□
進捗管理							
共通基盤システムの進捗管理	◎	◆	○□	△			
個別機能システムの進捗管理	◎	◆	△	□			
統合業務としての進捗管理	◎	◆	○□	△	△	△	△
品質管理							
共通基盤システムの品質管理	◎	◆	○□	△			
個別機能システムの品質管理	◎	◆	△	□			
統合業務としての品質管理	◎	◆	○□	△	△	△	△
問題・課題管理							
共通基盤システムの問題・課題管理	◎□	◆	○□	△			
個別機能システムの問題・課題管理	◎□	◆	△	□			
統合業務としての問題・課題管理	◎	◆□	○□	△	△	△	△
変更管理	◎□	◆□	○□	□	□	□	□
構成管理	◎	◆	○□	□	□	□	□
調達計画作成と調達の実施							
調達計画書の改訂	◎□	□	△				
調達仕様書の作成と調達実施							
工程管理支援事業者の調達	◎□						
共通基盤事業者の調達	◎□	◆□					
個別機能事業者の調達	◎□	◆□	□△				
ハードウェア等の調達	◎□	◆□	△	△			
運用事業者の調達	◎□	◆□	△	△			
ソフトウェア保守事業者の調達	◎□	◆□	△	△			
設計・開発業務							
基本的事項の整理	◎	◆	□				
共通基盤システムの設計・開発業務	◎	◆	□	△			
個別機能システムの設計・開発業務	◎	◆	△	□			
統合業務の実施	◎	◆	○□	□	□	□	□
全事業者が共同で実施する作業の推進							
結合テスト	◎	◆	○□	□	△		
総合テスト	◎	◆	○□	□	△	□	

凡例
◎：承認または確認
◆：検証支援
○：協働依頼及び取り纏め
□：実施
△：支援
無印：必要に応じ参加

主要業務	調達担当課室	工程管理 支援事業者	共通基盤 事業者	個別機能 事業者	ハードウェア 等納入事業者	運用事業者	ソフトウェア 保守事業者
受入テスト	◎□	◆□	△	△	△	△	△
各種マニュアルの作成							
・運用マニュアル	◎	◆	○□	□	△	△	△
・ユーザーマニュアル	◎	◆	○□	□	△	△	
研修	◎	◆	○□	□	△	△	
テスト環境の構築と運用	◎	◆	○□	□	□	△	△
本番運用環境の構築	◎	◆	○□	□	□	△	△
移行に関する業務	◎	◆	○□	□	△	△	△
サービスレベル合意書（SLA）の作成	◎	◆	○□	△	△	□	△
運用事業者への引継ぎ	◎	◆	○□	□	△	□	
ソフトウェア保守事業者への引継ぎ	◎	◆	○□	□			□
・・・・・・							

6.4.運用

6.4.1.調達分野の定義

ここで指す運用とは、情報システムの運用業務を行うための役務調達を指している。

尚、運用業務の調達においては、ヘルプデスク業務が含まれる場合がある(ヘルプデスクのみを独立して調達する場合もある)が、今回の「6.4.運用」の項ではヘルプデスク業務に関しての説明は行っていない。

運用業務を調達する際に、ヘルプデスク業務についても同時に調達を行う必要がある場合は、本項と併せて「6.5. ヘルプデスク」の項を参照の上仕様書を作成することが望ましい。

図 6.4-1 役務調達の分類における対応箇所

6.4.2 仕様書に記載すべき役務内容

6.4.2.1.代表的な役務作業の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務内容	役務の概要	SLCP のアクティビティ	調達基本指針に対応する仕様書の章・節（及びそのタイトル）
1.運用計画の策定	運用の実施計画を策定し、運用計画書を作成。府省担当者の承認を得る。	1.7.1.1 運用プロセス実施計画書の作成	10.運用要件定義
2.運用のための引継ぎ	システム開発事業者、既存の運用事業者（既存システムの場合）、導入業者等から説明を受けると共にドキュメントの提供を受ける。	1.7.1.2 運用のための資産の引継ぎ	9.移行要件定義 (1) 移行に係わる要件
3.運用環境の構築	システム運用に必要となる什器のうち、受注者が準備すべき什器の調達･設置を行う。	3.3.3　環境の構築	10.運用要件定義
4.運用要員の教育	システム運用者への訓練を行う。引継ぎの場合は、現行の運用事業者から研修･教育を受ける。また、故障対応訓練･セキュリティ研修等を実施する。	1.7.2.4 システム運用の訓練	9.移行要件定義 (2)教育に係わる要件
5.システム運用	システム運用に必要となる運用業務を実施する。 ・システム運用監視 ・サーバ機器類の監視 ・ネットワークの監視 ・ジョブ監視 ・ログ監視	1.7.4.1 システムの運用 1.7.4.2 運用監視及び運用データの収集、問題の識別、記録及び解決、運用環境の改善 1.7.4.3 問題の識別及び改善	10.運用要件定義

	・資源配布 ・バックアップとリストア ・媒体管理、消耗品管理 ・インシデント管理 ・問題管理 ・変更管理 ・リリース管理 ・構成管理 ・キャパシティ管理 ・ITサービス継続性管理 ・可用性管理 ・問い合わせ対応	1.7.4.4 運用環境の改善	
6.サービスレベル管理	サービスレベルの報告、改善	1.7.7 システム運用の評価	10.運用要件定義
7.運用会議の開催	定例会議体などで業務報告を行う。必要に応じて課題と解決方法に関する検討を行う。(月次、週次、年次、緊急報告会等 府省による)	1.2.6 レビュー及び評価	10.運用要件定義

6.4.2.2.各役務内容に関する説明及び仕様書上の記載例

1. 運用計画の策定

項目	内容
役務内容の概要	運用の実施計画を策定し、運用計画書を作成した上で、府省庁担当課の承認を得る。
想定されるインプット （発注者側で用意）	全体スケジュール 運用要領 運用設計書 体制図（当該システムの関連事業者、発注者） 役割分担（当該システムの関連事業者、発注者） 運用対象システムの概要 運用対象システムの構成情報 担当運用業務の内容・業務量等の要件 等
成果物 （受注者側で用意）	運用計画書 体制表　等 （府省庁によっては導入計画書、体制表等ドキュメントを分けて提出を求める場合も存在する。こうした点に関しては各府省庁で定められている調達方針・ガイドラインに沿う事が望ましい。）
仕様書に記載すべきポイント	設計・開発事業者、現状の運用事業者と調整の上、以下の内容を含む運用作業の実施計画を策定する **【1.基本的に記載すべき要求要件】** ・実施すべき作業内容 ・実施体制における役割分担、指示・命令系統 ・作業時間帯、作業場所等に関する指定及び制約条件 ・担当者に求められる要件（スキル・経験・資格） ・担当者の届出、変更の場合のルールの遵守 等 **【2.案件の種類・特性によって追記すべき要求要件】** ・運用環境構築等、付帯業務が発生する場合当該業務に関する計画
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○実施体制等 ① 受託者は落札決定後 7 日以内に運用計画書(スケジュール､実施体制 等を含む)を作成し､主管課に納入の上､承認を得ること。 ② 受注者は、本業務の実施に当たって、本業務に従事する運用支援要員２名以上、運用支援要員をサポートする補助要員２名以上の実施体制を整備し、その体制表に運用支援要員及び補助要員の所属・役職・氏名・連絡先を添えて担当職員に提出すること。 ③ 運用支援要員及び補助要員は、○○課に常駐し、本業務を実施す

	ること。 ④ 受注者は、受注者側の事情により、運用支援要員及び補助要員を変更する場合は、変更する日の 2 週間以上前までに担当職員と協議すること。 ⑤ 運用支援要員及び補助要員の変更を行う場合、受注者は引継書を作成し、十分な引継ぎ、トレーニングを行い、業務に支障を来さないようにすること。
案件・情報システムの特性等による留意点	① 設計・開発事業者において運用計画を策定しているケースも存在する。その場合、設計開発事業者と調整の上計画を確定させる必要あり。 ② 継続や追加調達等、既存の運用事業者との調整や既存の運用計画との連携・調整が必要な場合はその旨を記載する必要あり。 ③ 作業場所が複数にわたる場合や再委託が必要な場合などにはその旨を記載し、役割分担や責任範囲を明確にする。
セキュリティに関する留意点	① 体制図等に個人情報の記載がある場合、当該文書は規程に定める重要度に応じた取り扱いとする。

2．運用のための引継ぎ

項目	内容
役務内容の概要	受注者の運用担当者は、現行の運用事業者もしくはシステム構築(設計・開発)を行った事業者からの研修に参加し、教育を受ける。また、受注者は、運用開始後に必要に応じてセキュリティ研修などを運用担当者に実施する。 また、業者交替などにより運用業務を終了する場合、新たに運用業務を行う運用担当者に対し、業務内容の申し送りや必要な研修などを実施する。
想定されるインプット （発注者側で用意）	前任事業者（新規システムの構築の場合は、システム構築事業者。以降同様）からの引継計画書 前任事業者からの引継ぎ資料
成果物 （受注者側で用意）	○引継ぎを受ける場合 運用引継実施報告書 ○引継ぎを行う場合 （後任事業者への）引継ぎ計画書（案)、引継ぎ資料
仕様書に記載すべきポイント	受注事業者が業務引継を受ける場合、および引継ぎを行う場合の要求要件について記載する。 **【1.基本的に記載すべき要求要件】** ・前任事業者からの引継ぎ要件 ・後任事業者への引継ぎ計画の策定、引き継ぎ資料の作成 ・その他関連事業者との調整、説明、研修等への対応
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○引継ぎを受ける場合 （関連事業者との調整、引継計画書の作成） ① 本調達事業者は、運用対象システムの運用業務を遂行するために必要な情報をとりまとめるために、関連事業者と協議し、○○省が提示する「運用手順書」を考慮した上で「引継計画書」を作成すること。 （研修等への対応） ① 本調達事業者は、運用テストの開始前までに、システム運用担当者向けの研修を受講し、システム運用担当者向けの利用者マニュアルを熟読し、運用体制を整備すること。 ○引継ぎを行う場合 ① 平成ｘｘ年度以降の運用業者は別途調達を行う予定である。したがって、落札者は、平成ｘｘ年度以降の運用業務の落札者（以下「次

	期落札者」という。）が異なる場合、本業務の委託期間内に、落札者の負担と責任において、運用業務を滞りなく行えるよう次期落札者に対し確実に引継ぎを行うこと。 　また、引継ぎに当たり、以下の点を遵守すること。 ア　引継ぎの際は、引継責任者名及び引継内容等について、事前に当局に報告を行い、承認を得ること。 イ　引継ぎの際は、契約期間中に実施した作業の概要等を記載した「引継書」を作成し、当局の承認を得た後、当該「引継書」を利用して、次期落札者への引継ぎを行うこと。なお，平成ｘｘ年３月３１日までに作業が完了しない事案の詳細及び作業の進ちょく状況等については、別途「引継書」に追記すること。 ウ　引継ぎ計画書に基づき、引継ぎを行った結果について、当局の承認を得ること。なお、承認を得られなかった場合には、落札者の負担と責任において、引継期間を延長して業務に支障がないよう対応すること。
案件・情報システムの特性等による留意点	① 受注者が運用作業の準備を行うにあたって、調整を行うべきステークホルダーが複数に渡る場合、受注者が調整・説明を受ける対象事業者を明示する必要がある。 ② 次期運用事業者が決定した時点で現行運用事業者の委託期間が完了している場合､現行保守事業者から次期保守事業者へのハンズオンによる引継ぎは実施されず､発注者からの運用関連図書等の引き渡しを持って運用引継ぎを代替する必要がある。
セキュリティに関する留意点	－

3.　運用環境の構築

項目	内容
役務内容の概要	システム運用に必要となる什器のうち、受注者が準備すべき什器の調達・設置を行う。
必要となる インプット （発注者側で用意）	手配対象機器一覧 （すでに運用業務の受注者で手配する機器が定義されている場合）
成果物 （受注者側で用意）	作業報告書（環境構築）
仕様書に記載すべきポイント	システム運用事業者が什器等を手配する必要がある場合は、その旨を仕様書に記載する。実際に必要な什器等が決まっている場合はその型式等を明示する。 **【1.基本的に記載すべき要求要件】** ・仕様書の要求要件から適切な機器・ソフトウェアを選定 ・必要となる現地調査 ・現地調査を実施した結果、設計・作成すべき図面等のアウトプット ・現地調査の実施及びアウトプット提出のタイミング ・現地調査実施にあたっての制約事項 ・現地設置の際の設置スペースや電源容量 ・現地設置の際のインターネット回線、監視用回線接続有無　等
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○仕様書の要求要件から適切な機器・ソフトウェアを選定 ① 受注者は、運用管理業務に必要だと判断した什器類は受注者の負担で用意すること。什器類の例としては、机、椅子、棚、コピー機、FAX、情報管理に必要なハードウェアおよびソフトウェア、電話回線、インターネット回線等である。インターネット回線を敷設する場合は省内 LAN に接続してはならない。 　イ．受注者は、什器類の搬入･設置作業をするための申請を行うこと。 　ロ．受注者は、什器類の搬入・設置を行うための事前調査を行うこと。 　ハ．受注者は、搬入・設置作業に際し必要となる部材等の手配を行うこと。 　ニ．受注者は、什器類の梱包物、搬入の際に使用した養生品及びその他不要となった資材を、設置完了後速やかに撤去し廃棄すること。なお、環境への影響を考慮し、廃棄物は極力削減するように考

	慮すること。 　ホ．受注者は、搬入・設置作業については、基本的に平日の業務時間内に実施すること。詳細は別途、〇〇省より指示することとする。
案件・情報システムの特性等による留意点	① 調達すべき機器の手配・設置主体等の役割分担を明示する必要がある。
セキュリティに関する留意点	－

4. 運用要員の教育

項目	内容
役務内容の概要	現行の運用事業者、もしくはシステム構築（設計・開発）を行った事業者からの教育・研修に参加し、運用担当者を教育する。
想定されるインプット （発注者側で用意）	運用手順書
成果物 （受注者側で用意）	運用手順書（修正版） 作業報告書（要員教育）
仕様書に記載すべきポイント	システム運用担当者に対して実施すべき教育内容を記載する **【1.基本的に記載すべき要求要件】** ・受講すべき研修 ・実施すべき教育・訓練の内容 **【2.案件の種類・特性によって追記すべき要求要件】** ・セキュリティ研修等、運用開始後に定期的に運用担当者に実施すべき研修
仕様書記載上の例/説明	**仕様書に記載する主な作業内容** ○受講すべき研修 ① システム運用担当者向け研修の受講 　関連調達事業者は、システム運用担当者に対して、システム運用上必要となる設定方法及び操作方法に関する研修を、各システムの運用開始前までに実施することとなっている。 本調達事業者は、これらの研修に参加し、その内容を習得すること。 （以下略）
案件・情報システムの特性等による留意点	① 後任事業者が決定した時点で前任事業者の委託期間が完了している場合、前任事業者から後任事業者へのハンズオンによる引継ぎは実施されず、発注者からの運用関連図書等の引き渡しを以て要員教育に代替する必要がある。
セキュリティに関する留意点	―

5．システム運用

項目	内容
役務内容の概要	設計・開発事業者、又は既存の運用事業者から引き継いだ運用要領、運用手順書、運用ツールを用いて、必要となる運用業務を遂行する。
想定されるインプット （発注者側で用意）	運用設計書 運用要領 運用手順書 作業(変更・リリース)に関する申請・管理の為のドキュメント 府省庁で定めるセキュリティポリシー　等
成果物 （受注者側で用意）	運用報告書 作業報告書（運用作業） 運用手順書（追加・修正済みのもの）　等
仕様書に記載すべきポイント	システム運用に必要となる運用業務を遂行する。対象となる情報システムの運用業務要件、受注者が担う役割等から受注者に依頼すべき業務を抽出し、仕様書中に明示する。また、各業務の実施のタイミングについても記載する。 また、各作業の実施にあたっては各府省庁のセキュリティポリシーを遵守することが前提となる。 ・システム運用監視 ・サーバ機器類の監視 ・ネットワークの監視 ・ジョブ監視 ・ログ監視 ・資源配布 ・バックアップとリストア ・媒体管理、消耗品管理 ・インシデント管理 ・問題管理 ・変更管理 ・リリース管理 ・構成管理 ・キャパシティ管理 ・IT サービス継続性管理 ・可用性管理 ・問い合わせ対応（※ヘルプデスクの詳細役務内容は 6.5 ヘルプデスクに記載） 　等
仕様書記載上の例/	**仕様書に記載する場合の例**

説明	○ 本番運用作業 　本調達事業者は、運用手順書の規定内容に準じて、次の事項を遂行すること。 ア 各システムの運用監視 (1)本調達事業者は、オンライン運転状況、バッチ処理の実施状況等を監視すること。 (2)定期保守・計画停止時においては、各システムを停止・起動すること。 イ サーバ機器類の監視 (1)本調達事業者は、iDC 及び本省等に設置されたサーバ機器類の稼働状況を監視すること。 (2)定期保守・計画停止時においては、サーバ機器類を停止・起動すること。 ウ ネットワークの監視 (1)本調達事業者は、○○省内の LAN、WAN、iDC 及び各拠点（本省と地方拠点）に敷設されたネットワークの運用状況を監視すること。 エ ジョブ監視 (1)本調達事業者は、各システムのジョブ実行を監視すること。 (2)バッチ処理が正常に実行されたかを確認すること。 (3)手動での起動を必要とするバッチジョブを、起動指示を示す書面に基づいて、ジョブオペレーションを実施すること。 (4)異常処理した場合には、運用手順書に従って、再実行、障害の解析・回復又は担当者への連絡を実施すること。 オ ログ管理 (1)本調達事業者は、各システムのログを管理すること。 (2)不正利用の有無、不正侵入検知、情報漏えい、可用性・信頼性・機密性、ハードウェア故障、ソフトウェア故障等に関するログデータを収集しており、○○省の担当者がログ分析する際には協力すること。 カ 資源配布 (1)サーバ及びクライアント PC へ、プログラム等のファイルは自動的に配布される方式となっている。本調達事業者は、臨時配布又は自動

	配布が失敗した等を理由に手動での資源配布が必要となった場合、配布指示を示す書面に基づいて、実行すること。 キ バックアップとリストア (1)バックアップ作業は、自動的に実行する方式となっている。本調達事業者は、臨時のバックアップ作業及び障害復旧のためにリストア（データの戻し入れ）が必要となった場合、本作業の指示を示す書面に基づいて、実行すること。 ク 媒体管理と消耗品管理 (1)本調達事業者は、規定された保管方法に則り、媒体の保管及び媒体の情報・保管日時等を記録すること。 ケ インシデント管理 (1)サービスデスク及びシステム監視で検知されたインシデント（システムの不具合、機器の故障、エラー・警告のメッセージの発生等）を一元的に管理すること。 (2)過去のインシデント情報を検索し、対応できる事象がある場合、回答又は解決方法を実施すること。 (3)過去のインシデント情報を検索し、対応できる事象がない場合、緊急度、優先順次、影響範囲等を考慮して、問題管理にエスカレーションすること。 コ 問題管理 ・障害の切り分け (1)インシデント管理からエスカレーションされた事象を問題として一元的に管理すること。 (2)関連事業者の責任分界点に従って、問題を切り分けること。 (3)必要に応じて、関連事業者に調査を指示し、召集して臨時の対策会議を開催すること。 ・障害の調査・復旧 (1)障害の切り分け後、障害の該当箇所を担当している関連事業者に対して、問題の原因を特定させ、復旧作業を指示すること。 (2)障害が復旧するまで、作業内容を監理し、復旧したことを確認すること。 (3)一連の障害対応をとりまとめること。 (4)早急に根本的に解決できない場合、一時的な対応を実施すること。かつ、恒久的な解決策を策定又は関連事業者に依頼すること。

	サ 変更管理 (1)○○省の担当者又は問題管理から提示される変更要求を受け取り、一元的に管理すること。 (2)変更要求に従い、変更によって発生する影響事項及びリスクを洗い出し、変更計画を策定すること。また、変更計画を○○省の担当者に確認すること。 (3)変更計画の確認後、プログラム修正を必要とする場合、テスト検証後にリリースの可否を判定すること。 シ リリース管理 (1)変更管理の活動で挙げられた、新しいハードウェア、新しいソフトウェア、新しいバージョンのソフトウェアのリリース要求を受け取り、一元的に管理すること。 (2)リリース計画を策定し、リリースを実施すること。○○省担当者と協議の上、ウイルス対策用パターンファイルの更新、オペレーティングシステム、ミドルウェア等のパッチ適用作業を実施すること。 (3)ハードウェア機器類の交換等、関連事業者が作業する際には、本調達事業者が協力して立会い、作業後の結果を確認すること。 ス 構成管理 (1)システムを構成する、ネットワーク・ハードウェア・ソフトウェア・設備・マニュアル、マニュアルなどの情報を記録、整理して、常に最新かつ完全な状態に保つようにすること。 セ サービスデリバリー 　中長期的なシステム運用管理に関する計画と改善に対応することであり、具体的には以下の項目を遂行すること。 (1)キャパシティ管理 性能悪化やリソース不足などの問題を未然に防ぐために、パフォーマンス及びリソースを監視、測定、データ収集、記録して、これらの事項を報告すること。 (2)利用状況の変化の傾向を見据えて、サーバの処理能力と台数、ネットワークの帯域などを適正に維持するように努めること。 ソ IT サービス継続性管理 (1)大規模災害時やデータ消失時に備えて、バックアップを実施して保管すること。 担当府省庁、及び関連事業者が適切な復旧計画を作成し、代替手段を用意する検討に協力すること。

	タ 可用性管理 (1)サービスを安定提供するために、品質及びセキュリティの強化に協力すること。
案件・情報システムの特性等による留意点	① 利用者からの問い合わせ対応業務として、ヘルプデスクを設置する必要がある場合は「6.5 ヘルプデスク」を併せて参照すること。
セキュリティに関する留意点	―

6．サービスレベル管理

項目	内容
役務内容の概要	締結したサービスレベル合意書（SLA）に基づき、運用業務のサービスレベルについて府省庁に報告を行う。
想定されるインプット （発注者側で用意）	サービスレベル項目／定義書 サービスレベル合意書（SLA）
成果物 （受注者側で用意）	サービスレベル報告書
仕様書に記載すべきポイント	締結したサービスレベルの項目について、状況を管理・報告し、未達成の場合には改善を行う。 **【1.基本的に記載すべき要求要件】** ・サービスレベル項目の現状報告と評価
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇サービスレベル項目 ① サービスレベル管理 締結した「サービスレベル評価項目と要求水準」「サービスレベル評価方法」に基づき、サービスレベルの達成状況に関する報告を行うこと。なお、サービスレベルが未達成の場合には、あわせて「サービス改善計画」を具体的に提案すること。 〇サービスレベル合意書締結に関する記載例 本業務の実施に当たっては、当局と落札者の間で、SLA（サービスレベル合意書）を締結する。サービスレベル評価項目と要求水準については、以下に記載している要件を基本として、締結後当局と落札業者との協議により決定するが、協議の前提として「サービスレベル評価項目と要求水準」「サービスレベル評価方法」「未達成時のサービス改善計画」について具体的に提案すること。 1.正常稼働 (1)〇〇業務に関する業務データの完全性を担保できない事象(データの改ざんなど)の発生が0件であること。ただし、落札者の責任に帰するものを対象とし、他業者の責任に帰するものやリカバリの実施などにより業務に支障のない状態とした場合は発生件数の対象外とする。 (2)各システムごとの稼働率が 99.9%以上であること。ただし、落札者の責によらない事由に起因するシステム停止時間は対象外とする。

	(3)障害窓口業務の年間サービス稼働率（受付件数全体に対する適切な対応を取った件数の割合。例えば、管理体制や対応マニュアルの設計不備により、不適切な対応が発生した回数を記録すること等を想定している）が 99.9%以上であること。 2.サービス品質 (1)本業務の実施に当たり、落札者の負担のもと、〇〇業務の内容理解に努め、システムの開発・保守を行う業者と調整して、〇〇システムの機能の理解に努めること。 (2)落札者は、落札者の負担のもと、導入するハードウエア、ソフトウエア製品を納入している業者と調整して、製品の理解に努めること。 (3)落札者は、次期システムの周辺システムを含む、ネットワーク構成全体について理解に努めるとともに、本システムが周辺システムと合わせて連携して稼働すべきものであることに留意すること。 (4)本業務の実施に当たり、落札者の責任に起因して、切り替え業務及び正常な運用業務の提供がなされなかった場合、又はシステムおよび〇〇業務データに影響やトラブルを与えた場合には、落札者の負担と責任において対応すること。 (5)当局は、落札者が本業務を履行する上で必要な関係書類を随時貸与する。ただし、貸与された書類は、当局から請求があった場合及び履行期間終了後に当局に返還すること。 <<略>> (9)落札者は、作業に際して必要な都度、当局に状況を報告し相談しながら問題にあたること。 (10)以上に反した場合には、報告書の提出を求めたうえ、SLA ポイントに加算することもある。
案件・情報システムの特性等による留意点	〇サービスレベル合意書締結時の留意点 ① 運用調達はサービスの購入であることから、評価指標としてサービスレベル合意書（SLA）を締結する必要がある。システムの非稼働は調達したそのハードウエア・ソフトウエアなどによって引き起こされることが多く、必ずしも運用の責任ではない。またシステム障害時のバックアップ発動による非稼働時間の短縮などはアーキテクチャによって違いが生ずる。それらを加味した上で運用の評価としてのサービスレベル値の設定・評価が必要となる。 ② 運用報告や監視の質についても評価を行うことが望ましい。 ③ サービスレベル項目達成の実績に従ってペナルティを課す考え方がある。成功報酬として、「支払金額（落札金額）＝基本報酬＋成功報酬」の考え方を基に、発注者と落札者の間で合意したサービスレベル項目の達成状況に応じて支払金額を決定する。なお、一般的

	に落札者は、発注者との間で合意した事項に対し不履行が発生した場合に、損害賠償などの責任を負うことは社会通念上の義務として認識されるべきものであるが、発注者の最大の希望は、落札者から品質の高いサービスが提供されることにあり、報酬の考え方はそのための工夫として設定するものである。落札者に不当に厳しい条件を科すことを目的とするものではない。 　条件例(1)　基本報酬と成功報酬の割合は 9:1 とする。 　条件例(2)　成功報酬の配分割合は以下とする。 　　(2-1) 10%（満額）　全サービスレベル項目で指定条件達成 　　(2-2)　5%　指定条件を達成できない項目が全体の 5%未満 　　(2-3)　2%　指定条件を達成できない項目が全体の 5%以上 10%未満 　　(2-4)　0%　指定項目を達成できない項目が全体の 10%以上
セキュリティに関する留意点	―

7．運用会議の開催

項目	内容
役務内容の概要	運用会議等を開催し､府省の担当課室に業務報告を実施する。必要に応じて課題と解決方法に関する検討を実施する。 （月次、週次、年次、緊急報告会　等）
想定されるインプット （発注者側で用意）	運用会議開催日程（案）
成果物 （受注者側で用意）	日報 週報 月報 臨時対策会議報告書 運用報告書 運用会議議事録
仕様書に記載すべきポイント	定例の会議体、開催時期、提出する報告書、報告内容等必要なレビューとタイミング、その方法について記載する。 **【1．基本的に記載すべき要求要件】** ・会議名 ・参加者 ・提出する報告書名 ・報告すべき内容
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇運用会議の開催 本調達事業者は、次に示す会議を開催すること。各会議で報告書を作成すること。 なお、必要に応じて関連事業者の参加を〇〇省の担当者に確認した上で要請することができる。 ①日次運用会議 ・参加者　：本調達事業者 ・開催時期：開庁日及び点検等のために休日出勤した日 ・報告書名：日報 ・報告内容 - 前日のインシデント及び故障の発生と対応状況（発生・仕掛・完了の件数） - 前日のヘルプデスクの対応状況（問合せ件数） - 前日のシステムの運用状況（サービス開始・終了時間、運用作業

	の内容・時刻・担当者・確認者） - 当日の運用作業の予定　等 ②週次運用会議 ・参加者　：〇〇省の担当者、本調達事業者 ・開催時期：週次 ・報告書名：週報 ・報告内容 - １週間のインシデント及び故障の発生と対応状況 （発生・仕掛・完了の件数、進捗状況） - １週間のヘルプデスクの対応状況（問合せの総件数、傾向、分布） - １週間のシステムの運用状況の概要 - 翌週の運用作業の予定・計画　等 ③月次運用会議 ・参加者　：〇〇省の担当者、本調達事業者 ・開催時期：月次 ・報告書：月報 ・報告内容 - １ヶ月間のインシデント及び故障の発生と対応状況（発生・仕掛・完了の件数、進捗状況） - １ヶ月間のヘルプデスクの対応状況（問合せの総件数、傾向、分布） - １ヶ月間のシステムの運用作業の概況（問題、変更の状況） - １ヶ月間のサービスレベルの達成状況及び - １ヶ月間の性能監視の結果 - １ヶ月間のリソースの利用状況 - １ヶ月間のセキュリティ状況（不正アクセス検知数、ウイルス検知数、改ざん検知数、不正メール検知数、ユーザ数の増減、アカウントロック数、脆弱性に関する新着情報） - 当月の運用作業の予定・計画（工事含む）　等 ④構成管理の棚卸状況報告会 ・参加者　：〇〇省の担当者、本調達事業者 ・開催時期：半期毎 ・報告書名：構成管理棚卸表 ・報告内容：サーバ機器類、ソフトウェア等のシステムの構成状況の結果

	⑤臨時対策会議 ・参加者　：〇〇省の担当者、本調達事業者 ・開催時期：随時（緊急性の高い問題が発生した場合） ・報告書名：臨時対策会議報告書 ・報告内容：事象及び問題に関する報告、確認、分析、検討等の結果
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	－

6.4.3.納入成果物と提出のタイミング

納入成果物とタイミングを記載すると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	納入成果物	納入期限
1. 運用計画の策定	運用計画書 体制表	契約後定められた期日内、変更した場合は随時
2. 運用のための引継ぎ業務	〇引継ぎを受ける場合 運用引継実施報告書 〇引継ぎを行う場合 （後任事業者への）引継ぎ計画書（案）、引継ぎ資料	引継ぎ完了後１週間以内 引継ぎ実施前
3. 運用環境の構築	作業報告書（環境構築）	機器導入前 環境構築時 環境構築作業終了時
4. 運用要員の教育	運用手順書（修正版） 作業報告書（要員教育）	研修受講後 研修受講後
5. システム運用	運用報告書 作業報告書（運用作業） 運用手順書（修正済みのもの）	日時、週次、月次、年次 随時 修正後提出
6. サービスレベル管理	サービスレベル報告書	定められたタイミング
7. 運用会議の開催	日報 週報 月報 臨時対策会議報告書 運用報告書 議事録	日次 週次 月次 随時 定められたタイミング、最終納品時 会議後定められた期日内

6.4.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	インプット	インプットを提示する タイミング
1.運用計画の策定	全体スケジュール 運用要領 運用設計書 体制図（当該システムの関連事業者、発注者） 役割分担（当該システムの関連事業者、発注者） 運用対象システムの概要 運用対象システムの構成情報 担当運用業務の内容・業務量等の要件	入札公示時応札期間中 応札期間中 入札公示時
2.運用のための引継ぎ	前任事業者（新規システムの構築の場合は、システム構築事業者。以降同様）からの引継計画書 前任事業者からの引継ぎ資料	契約締結後
3.運用環境の構築	手配対象什器等	入札公示時
4.運用要員の教育	運用手順書	入札公示期間中、応札予定者に閲覧を許可する。また、落札者には契約締結後貸与を行う。 契約締結後
5.システム運用	運用設計書 運用要領 運用手順書 作業（変更・リリース）に関する申請・管理の為のドキュメント 府省庁で定めるセキュリティポリシー	入札公示期間中、応札予定者に閲覧を許可する。また、落札者には契約締結後貸与を行う。
6.サービスレベル管理	サービスレベル項目／定義書 サービスレベル合意書（SLA）	入札公示時 契約締結時
7.運用会議の開催	運用会議開催日程（案）	入札公示時

項番	サービスレベル項目	規定内容	単位
1	運用サービス提供時間帯	運用サービスを実施する時間帯	時間帯
2	運用サービス提供状況の報告方法／間隔	運用状況･運用予定の報告方法／時間間隔	時間
3	バッチ処理時間	バッチ処理に費やした時間	時間
4	物理資源監視頻度	パフォーマンスなど物理資源の監視震度	回／日
5	障害通知プロセス･通知時間	運用障害発生時の連絡プロセスの有無と通知までの時間	有無 時間
6	バックアップ取得	バックアップの取得内容･方式･頻度	有無
7	バックアップ時間	バックアップ取得に必要な時間	時間
8	バックアップデータの 保存期間	バックアップした媒体の保存期間	時間
9	バックアップ復旧時間	システム停止時間からデータ復旧までの時間	時間
10	ログの取得	利用者に提供可能なログの取得内容･方式･頻度	有無
11	ログの保存期間	ログを保存した媒体の保存期間	時間
12	障害復旧	障害発生時のシステム復旧／サポート体制	有無
13	運用環境整備／撤去時間	運用サービスを実施するための環境整備に必要な時間／運用環境を撤去するための時間	時間
14	要員教育時間	運用要員などに対する各種教育に費やす時間 業務開始時、定期的な研修など	時間
15	報告	定例報告	項目

表 6.4-2 サービスレベル項目の例

6.4.5.役割分担

運用事業者と府省庁、その他業務の調達事業者との役割分担について、ここでは一例を紹介する。

分離・分割調達では分離発注の範囲、府省庁における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。
調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表を作成することが必要である。

○：主担当、△：支援、助言

作業項目	主管課	運用 事業者	引継運用 事業者 ※1	関連 事業者 ※2
1. 運用計画の策定	△	○		△
2. 運用のための引継ぎ		○	△	
3. 運用環境の構築		○		△
4. 運用要員の教育		○		△
5. システム運用		○		△
6. サービスレベル管理	△	○		△
7. 運用会議の開催	△	○		△

※1 引継運用事業者： 運用引継ぎを受ける、又は運用引継ぎを行う事業者
※2 関連事業者： 保守（ハードウエア、ソフトウエア）事業者、iDC 事業者、ヘルプデスク事業者など運用事業者と連携する事業

6.5.ヘルプデスク

6.5.1.調達分野の定義

ヘルプデスクの調達は、情報システムの運用においてユーザからの問い合わせに適切な応対（1 次回答、2 次エスカレーション、データ登録、FAQ 管理等）ができるようなヘルプデスク環境を構築し運用する役務作業の調達を指す。

ヘルプデスクの調達においては、運用役務作業を全体的にマネジメントする事業者は別途調達され、ヘルプデスクが個別調達されるケースと、運用事業者がヘルプデスク業務を運用役務作業の一部として包括的に受託するケースがそれぞれ存在する。後者のケースにおいては、ヘルプデスク業務部分は本章が該当し、その他の運用役務作業は「6.4.運用」を参照する必要がある。

なお、ヘルプデスクの個別調達は、大規模システムを対象とするものがほとんどである。小規模のシステムの場合は、運用の一環として調達される場合が大半である。

また、役務調達の分類の中では、下図に示すように、運用･保守フェーズにおける調達分野の１つである。

図　6. 5-1　役務調達の分類における対応箇所

6.5.2.仕様書に記載すべき役務内容

6.5.2.1.代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [9]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[10]の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務作業の概要	共通フレーム 2007 のアクティビティ	調達基本指針に対応する仕様書の章･節（及びそのタイトル）
1. 運用計画の策定	ヘルプデスク業務の実施計画、導入計画及び業務運用計画を作成し、計画書として提出した上で府省庁担当課などからの承認を得る。また、作業進捗状況において必要に応じて定期的なレビュー･計画の変更等を実施する	1. 7. 1. 1 運用プロセス実施計画書の作成	10 章　運用要件定義 （および、要約を 2 章(5)　作業内容･納入成果物へ記載
2. 運用のための引継ぎ業務	統括責任者、前年度ヘルプデスク運用事業者等から説明および必要なドキュメントの受領 次の業者への引継ぎ計画および引き継ぎ資料の作成 引継ぎを実施	1. 7. 1. 2 運用のための資産の引継ぎ	
3. 作業環境の整備	ヘルプデスク業務に必要な、電話、FAX、PBX、CTI、各種サーバ、ソフトの用意や、回線引き込み	－	
4. サービスレベル管理	ヘルプデスク運用にあたって必要な SLA を締結するとともに、サービスレベルの報告	1. 7. 1. 9 業務運用評価基準の設定	
5. ヘルプデスク業務運用	一次受付、一次回答、エスカレーション 問い合わせ内容の記録と分析、FAQ 掲載内容の抽出と更新 ユーザ端末のリモート操作　等	1. 7. 6. 1 業務の運用 1. 7. 6. 2 利用者支援	10 章　運用要件定義 （および、要約を 2 章(5)　作業内容・納入成果物へ記載
6. 利用者満足度調査	システム利用者に対する満足度	－	

[9] 独立行政法人　情報処理推進機構　共通フレーム 2007
ソフトウェアライフサイクルプロセス　SLCP-JCF 2007
[10] 総務省　情報システムに関わる政府調達の基本指針　2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

役務作業	役務作業の概要	共通フレーム2007のアクティビティ	調達基本指針に対応する仕様書の章･節（及びそのタイトル）
	調査の実施と報告		
7.ヘルプデスク運用会議	定例会議体などでヘルプデスク業務の運用報告を行う。また、議事録の作成を行う。 必要に応じて課題と解決方法に関する検討（月次、週次、年次、緊急報告会　等） ヘルプデスク運用マニュアル、各種報告書を作成･提出	1.2.6 レビュー及び評価 1.7.1.5 システム運用に係わる作業手順の確立 2.1 文書化プロセス	

6.5.2.1.各役務内容に関する説明及び仕様書上の記載例

1．運用計画の策定

項目	内容
役務内容の概要	ヘルプデスク業務の実施計画、導入計画及び業務運用計画を作成し、計画書として提出した上で府省庁担当課などからの承認を得る。また、作業進捗状況において必要に応じて定期的なレビュー・計画の変更等を実施する
想定されるインプット （発注者側で用意）	・導入予定及び利用者の概算人数 ・役割分担 ・全体スケジュール（案） ・体制図（案） ・運用体制（案）
成果物 （受注者側で用意）	・実施計画書 ・ヘルプデスク環境構築図 ・導入計画書 ・運用計画書、運用実施要領 （府省庁によっては導入計画書、体制表等ドキュメントを分けて提出を求める場合も存在する。こうした点に関しては各府省庁で定められている調達方針・ガイドラインに沿う事が望ましい）
仕様書に記載すべきポイント	府省庁側で計画の妥当性を判断するために必要となる以下の要件について仕様書に記載すること。 その他、案件に応じて計画書として事前に提出を求める必要があるものに関しては要件として記載すること。 **【1.基本的に記載すべき要求要件】** ・業務実施計画の策定 ・導入計画の策定 ・業務運用計画の策定 ・運用管理 **【2.案件の種類・特性によって追記すべき要求要件】** ・運用と別調達の場合は運用事業者の運用計画との関係を明示する必要がある。
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇業務実施計画の策定 受託者は、あらかじめ業務実施計画の策定として、ヘルプデスク業務実施計画書（以下「業務実施計画書」という。）を作成し、〇〇省専任部門の承認を受けること。 以下に、業務実施計画の策定内容を示す。

項目	内容
	(1) 全体スケジュール (2) 成果物 (3) 計画の改定手順及び変更管理手順 ○導入計画の策定 受託者は、業務実施計画を策定の後、導入期間中の作業計画を示したヘルプデスク業務導入計画書（以下「導入計画書」という。）を作成し、○○省専任部門の承認を受けること。 以下に、導入計画の策定内容を示す。 (1)導入スケジュール (2)ヘルプデスク業務環境整備計画 (3)ヘルプデスク要員教育計画 (4)実施体制 (5)会議体 (6)要員計画（導入期間中分） ○業務運用計画の策定 (1)業務運用計画の策定 受託者は、本業務のサービス開始までに、サービス開始後のヘルプデスク業務運用について、ヘルプデスク業務運用計画書（以下「業務運用計画書」という。）を作成し、○○省専任部門の承認を受けること。 以下に、業務運用計画の策定内容を示す。 ①ヘルプデスク業務運用計画 ②実施体制 ③会議体 ④要員計画（サービス提供期間中） ⑤計画の改定手順及び変更管理手順 (2)業務運用実施要領の策定 受託者は、本業務のサービス開始までに、「○○関係業務情報システム 運用センター運用・保守要領（平成○○年（○○○○ 年）○○月）」（以下「運用・保守管理要領」という。）に基づき、ヘルプデスク業務運用実施要領（以下「業務運用実施要領」という。）を作成し、○○省専任部門の承認を受けること。 なお、業務運用実施要領の作成にあたっては、統括責任者及び運用サービス担当業者と調整を実施すること。また、エスカレーション時の流れ及び連絡手段の詳細についても、統括責任者及び運用サービス担当業者と協議の上、業務運用実施要領に反映すること。 以下に、作成する業務運用実施要領を示す。

項目	内容
	なお、作成する業務運用実施要領に過不足がある場合には、受託後に〇〇省専任部門と協議の上、決定すること。 ①文書管理実施要領 ②サービス指標管理実施要領 ③課題・問題管理実施要領 ④コミュニケーション管理実施要領 〇運営管理 受託者は、上記で策定した業務実施計画、導入計画及び業務運用計画に基づき、本業務の運営管理を行うこと。
案件・情報システムの特性等による留意点	運用と一括でヘルプデスクが調達される場合は、本項目のみでなく、6.4 運用 における計画策定役務作業の内容も加える必要がある。
セキュリティに関する留意点	情報セキュリティ対策実施要領の遵守

2. 運用のための引継ぎ業務

項目	内容
役務内容の概要	統括責任者、前任ヘルプデスク運用事業者等から説明を受けると共にドキュメントの提供を受ける 後任事業者への引継ぎ計画および引き継ぎ資料の作成を行い、引継ぎを実施する
想定されるインプット （発注者側で用意）	・前任事業者（新規システムの構築の場合は、システム構築事業者。以降同様）からの引継計画書 ・前任事業者からの引継ぎ資料、業務内容、運用作業、セキュリティ等に係る研修
成果物 （受注者側で用意）	・後任事業者への引継計画書 ・後任事業者への引継ぎ資料 ・引継実施報告書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・前任業者からの引継ぎ要件 ・後任業者への引継ぎ計画の策定、引継ぎ資料の作成 **【2.案件の種類・特性によって追記すべき要求要件】** ・FAQ などのデータ引継ぎが発生する場合は、データ引継ぎのための要件記述
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○前任者からの引継ぎ ヘルプデスクのノウハウ等の本運用の業務に必要な事項について統合運用監視（移行中）事業者から引継ぎを受ける。本システムに関連するデータの引継ぎを受ける。また、引継ぎ計画書の作成と、引継ぎ完了報告書の作成を行う。 (1)前任業者からの引継作業 ①受注者は、本システムの運用業務を実施するために必要な情報について、統合運用監視（移行中）事業者の指示にしたがい、「引継計画書」を作成すること。また、引継作業の完了時に「引継完了報告書」を作成すること。概略スケジュールを「統合運用監視の準備と引継」に示す。 ②受注者は、統合運用監視（移行中）事業者が本番の統合運用監視業務を実施中に、統合運用監視（移行中）事業者からの引継と環境の準備をしなければならない。受注者は、統合運用監視（移行中）事業者の運用業務を滞らせてはならない。 ③引継は、受注者が主体的に行う必要がある。下記の点に留意して引継を実施すること。 （ア）設計書や運用に関する文書等からシステム構成や運用

項目	内容
	内容を自主的に習得すること。 （イ）統合運用監視（移行中）事業者へ質問する場合は、設計書や運用に関する文書等を十分に理解した上で行うこと。 （ウ）統合運用監視（移行中）事業者と協議の上、統合運用監視（移行中）事業者の運用業務に支障が出ないような問い合わせや質問の方法を決定すること。 ④データ引継 受注者は、本システムに関する下記のすべてのデータを統合運用監視（移行中）事業者から引き継ぐこと。また、受注者は引継いだデータを自ら理解するように努めること。 ・業務データ ・運用関連データ(インデント管理データ、ヘルプデスクの FAQ データ、構成管理データ等) ・ライブラリ管理システムに格納しているすべてのデータ(設計書、手順書、定義ファイル等) ・すべての台帳のデータ(バックアップテープ台帳、iDC 入退出者台帳等) ・その他(紙として存在するデータ、外部媒体に格納されているデータ等) 〇後任事業者への引継ぎ 後任事業者の契約締結後、速やかに、業務内容、運用作業、セキュリティ等に係る研修を行うこと。 なお、実運用を想定した引継ぎ作業を予定している。 (1)受注者は、契約終了前までに、運用作業に係る作業内容、結果等について次の業者に引継ぎを行うこと。 (2)受注者は、引継ぎを実施するに当たって、特定製品・技術に依存せず､次の業者がシステムの保守や拡張を引き継ぐことが可能であるようにすること。 (3)受注者は、引継ぎ計画の策定、引継ぎ資料の作成を行い、〇〇業務室の承諾を得ること。 (4)受注者は、引継ぎ期間、期限等について、〇〇業務室の指示に従うこと。 (5)受注者は、引継ぎ資料の作成漏れ等があった場合は、契約終了後においても次の業者からの質問に対する回答の対応等を行うこと。
案件・情報システム	新規開発の場合は、設計・開発事業者から引継ぎを受けることが好

項目	内容
の特性等による留意点	ましい。また、前任事業者からの引継ぎが困難な場合は主管課から引継ぎを受けることが好ましい。
セキュリティに関する留意点	－

3．作業環境の整備

項目	内容
役務内容の概要	ヘルプデスク業務に必要な、電話、FAX、PBX、CTI、各種サーバ、ソフトの用意や、回線引き込みなどを行う
想定されるインプット （発注者側で用意）	・回線の敷設における制約事項 ・ヘルプデスク運用マニュアル変更に必要となる、制度改正やシステム改修の詳細
成果物 （受注者側で用意）	・ヘルプデスク業務教育資材 ・ヘルプデスク業務マニュアル ・ヘルプデスク用電話回線 ・ヘルプデスク用電話回線の敷設図 ・音声応答サーバ用電話回線 ・音声応答サーバ用電話回線の敷設図
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ヘルプデスク環境の構築 ・回線の引き込み **【2.案件の種類・特性によって追記すべき要求要件】** ・ヘルプデスク業務の整備 ・ヘルプデスク業務マニュアルの作成 ・ヘルプデスク要員の教育 ・ヘルプデスク導入実施状況の報告 ・制度改正やシステム改修にともなうマニュアル等変更
仕様書記載上の例/説明	**仕様書に記載する場合の例** **【1.基本的に記載すべき要求要件】** ・ヘルプデスク環境の構築（業務に必要な、電話、FAX 、PBX、CTI、各種サーバ、ソフトの用意） (1)運用業務に必要な什器類等の準備 ①受注者は、運用業務に必要だと判断した什器類は受注者の負担で用意すること。什器類の例としては、机、椅子、棚、媒体格納キャビネ、コピー機、FAX、情報管理に必要なハードウェア及びソフトウェア、インターネット回線、電話回線等である。インターネット回線を敷設する場合は省内 LAN に接続してはならない。 ②受注者がヘルプデスク端末、運用管理端末の台数が不足と判断した場合は、必要に応じて〇〇局が準備した端末と同等のヘルプデスク端末、運用管理端末を準備すること。 ③受注者は、什器類の搬入・設置作業をするための申請を行う

項目	内容
	こと。 ④受注者は、什器類の搬入・設置を行うための事前調査を行うこと。 ⑤受注者は、搬入・設置作業に際し必要となる部材等の手配を行うこと。 ⑥受注者は、什器類の梱包物、搬入の際に使用した養生品及びその他不要となった資材を、設置完了後速やかに撤去し廃棄すること。なお、環境への影響を考慮し、廃棄物は極力削減するように考慮すること。 ⑦受注者は、搬入・設置作業については、基本的に平日の業務時間内に実施すること。詳細は別途、○○局より指示することとする。 (2)ヘルプデスク環境の構築 受注者は、ヘルプデスク設置場所及び環境を構築すること。リモート監視を実施するときには同時にリモート監視が可能な環境を構築すること。 さらに、○○庁舎から接続する回線を準備すること。 ○回線の引込み等に関する要件 (1)○○庁舎の運用作業場所で回線が必要な場合は、回線を引込む必要がある。 受注者は、回線の引込みに関する現地調査を実施すること。光ファイバ、LAN ケーブル等の配線経路の確認（床下、床上、縦管路、天井配管等）である。 (2)受注者は、引込み経路について、○○局の承認を得ること。 (3)受注者は、回線の引込み作業を実施すること。 (4)データセンターの運用作業場所は、回線の引込みは不可である。運用作業場所以外での通信手段を確保すること。費用は、受注者が負担すること。 **【2.案件の種類・特性によって追記すべき要求要件】** ○ヘルプデスク業務の整備 受託者は、ヘルプデスク業務の準備作業として、以下の作業を実施すること。また、その他必要となる作業がある場合には、受託者において作業を実施すること。 (1)FAQ 情報を参照する環境の準備

項目	内容
	○○システムでは、システム利用者向けに霞が関 WAN を経由して FAQ 情報の公開を行うこととなっている。受託者はこの FAQ 情報を参照することができないため、初期の FAQ 情報を○○省専任部門より受け取り、ヘルプデスク内でオペレータ等がこれを参照する環境を独自に準備すること。 なお、FAQ 情報に関する運用の詳細については、「システム利用者向け FAQ 情報に係る対応」を参照のこと。 (2)業務マニュアルの作成 受託者は、本業務のサービス開始までに、策定した業務運用計画及び業務運用実施要領に基づき、ヘルプデスク担当業者内部で必要となるオペレータの電話応対、ヘルプデスクシステム（注）の操作方法等に関するヘルプデスク業務マニュアル（以下「業務マニュアル」という。）を作成すること。 （注） 運用サービス担当業者及びヘルプデスク担当業者が○○システムの操作等を確認するための環境であり、擬似データを登録し○○システムと同じ業務アプリケーションを動作させる環境を示す。 ○ヘルプデスク要員の教育 受託者は、本業務を円滑に実施するために、サービス開始までに、オペレータ等のヘルプデスク要員に対して必要となる教育を受託者の責任において実施すること。 なお、ヘルプデスク要員の教育実施に当たっては、FAQ コンテンツ及び擬似環境を有効利用するとともに、教育マニュアル等の教育資材を作成し、受託者内において効率的かつ効果的な教育を実施すること。 ヘルプデスク要員の教育における教育内容及び○○省の支援について、以下に示す。 (1)教育内容 受託者において、以下の教育内容について、効率的かつ効果的な教育を実施すること。 ① ○○業務全体の内容 ② ○○システムの機能及び操作 ③ 運用実施要領の内容 ④ 業務マニュアルの内容 ⑤ 情報セキュリティ対策 ⑥ その他必要となる教育内容 ○ヘルプデスク導入実施状況の報告 ヘルプデスク導入作業の実施状況については、以降に示す会議にお

項目	内容
	いて、○○省専任部門へ報告すること。また、受託者内において、導入実施状況を確認するための会議等を随時実施し、状況把握に努めること。 なお、本業務のサービス開始に支障をきたすような緊急又は重大な問題が発生した場合には、速やかに○○省専任部門へ報告すること。 ○制度改正、○○システムの改修等による対応 受託者は、制度改正や○○システムの改修等に伴い、業務運用計画書、業務運用実施要領、マニュアル等の各文書の改定が必要となった場合には、○○省専任部門と協議の上、速やかに各文書の修正を行うこと。その際、必要に応じて、各文書の修正に必要となる○○システムの改修内容の詳細について、設計・開発担当業者から情報の提供を受けること。また、改定内容について、作業従事者への周知及び教育を徹底することで、情報共有を図り、本業務の遂行に支障をきたすことのないように努めること。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	ヘルプデスク要員教育 ➢ ヘルプデスク要員に対して、ヘルプデスク業務を行う際に、実施すべき情報セキュリティ対策に関して教育を実施すること。

4. サービスレベル管理

項目	内容
役務内容の概要	ヘルプデスク運用にあたって必要なSLAを締結するとともに、サービスレベルの報告を行う
想定されるインプット（発注者側で用意）	・サービスレベル項目／定義書
成果物（受注者側で用意）	・サービスレベル合意書（SLA） ・サービスレベル報告書
仕様書に記載すべきポイント	※運用と一括でヘルプデスクが調達される場合は、本項目のみでなく、6.4 運用　でのサービスレベル項目も加える必要がある。「6.5.4 想定されるインプット」では、ヘルプデスク運用のみを単独で調達した仕様書例におけるサービスレベル項目を挙げている。 **【1.基本的に記載すべき要求要件】** ・サービスレベル項目（稼働率、放棄率、バックログ率、再応答比率、目標応答時間、応答時間順守率、目標対応時間、対応時間順守率など） ・サービスレベル合意書（SLA)の作成 ・サービスレベル未達成時における対応
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○サービスレベル項目 本項目に関する要件は、次のとおりである。 (1)サービスレベル達成度合いの指標 調達事業者は次の表に示す各サービスレベル項目に対する達成状況を月単位で評価し、それらを 3 ヶ月毎に実施する「サービスレベル報告会」において、3 ヶ月分を集計した結果を〇〇省に報告すること。 受注者から報告される毎月のサービスレベル達成状況に、改善提案等の内容を加味した上で、調達事業者と〇〇省の協議に基づいて当該期間分のサービスレベルの達成度合いを確定する。 表：サービスレベル達成度合いの指標 達成度合い　　条件 A　　全サービスレベル項目で指定条件達成 B　　指定条件を達成できないサービスレベル項目が 3 ヶ月の合計サービスレベル項目数全体のうち 5%未満 C　　指定条件を達成できないサービスレベル項目が 3 ヶ月の合計サービスレベル項目数全体のうち 5%以上 10%未満

項目	内容
	D　　指定条件を達成できないサービスレベル項目が 3 ヶ月の合計サービスレベル項目数全体のうち 10%以上 (2)サービスレベル達成度合い向上のための措置 調達事業者側原因によるサービスレベル未達成項目がある場合、調達事業者は以下に示すような措置を通じて、達成度合いの向上に努めること。 ①無償による対応 調達事業者の責により SLA が遵守できなかった場合､その改善策（手続き見直し、仕組み・ツールの導入、試験・検証など）の検討・実施を必須とし、必要とする作業は調達事業者の負担により無償で行うこと。 ②体制の見直し・主要担当者の専任化 「達成度合い C」以下の状況においては、調達事業者は主要担当者（責任者及び補佐など）を本契約以外の業務に従事させてはならない。 (3)サービスレベルの達成が困難な状況が続く場合の措置 調達事業者側原因によりサービスの品質が著しく低く、改善が期待できない場合等においては、報酬を減額することがある。 ○サービスレベル合意書（SLA)の作成およびサービスレベル協定の締結 受託者は、サービスレベル定義書（案）を踏まえ、サービス開始の 1 ヶ月前までに、○○省専任部門に対して提供できるサービスレベル項目及びその指標を明らかにしたサービスレベル合意書（SLA)を作成し、○○省専任部門とサービスレベル協定（以下「SLA」という。）を締結すること。また、受託者は、締結した SLA を遵守すること。 ○サービスレベル未達時の対応 なお、サービスレベル合意書（SLA)では、サービスレベル未達成時における対応として、サービス指標の見直し、契約内容の見直し等の対応についてあらかじめ定めておくものとする。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	－

5．ヘルプデスク業務運用

項目	内容
役務内容の概要	一次受付、一次回答、エスカレーション 問い合わせ内容の記録と分析、FAQ 掲載内容の抽出と更新 ユーザー端末のリモート操作　　など
想定されるインプット （発注者側で用意）	－
成果物 （受注者側で用意）	・FAQ 情報 ・稼動状況報告書 ・問い合わせ・対応履歴情報 ・日報 ・週報 ・月報
仕様書に記載すべきポイント	**【１．基本的に記載すべき要求要件】** ・一次受付、一次回答、エスカレーション －受付時間 －一元的な窓口対応 －エスカレーション －一次回答 －ヘルプデスクでの問い合わせ対象 ・問い合わせ内容の記録と分析、FAQ 掲載内容の抽出と更新 ・問合せ完了要件
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○一次受付、一次回答、エスカレーション ⑴原則として、窓口の受付時間は休日（行政機関の休日に関する法律第１条に定める日）を除き 9 時から 18 時までとし、FAX・電子メールの受付は 24 時間受け付けられるものとする。 ただし、受付の時間帯が短縮又は数日間中止としたい場合、調達事業者はその旨を事前に連絡し、○○省がこれを認めた場合に限り、前述の時間帯の制約は除かれるものとする。 ⑵○○省の職員からの電話又は FAX、電子メールでの各種問い合わせに対して、一元的な窓口として対応すること。 ⑶問い合わせ内容が、ヘルプデスクで回答可能な内容かどうかの判断と、回答可能な場合は１次回答を行い、回答できない場合には２次エスカレーションをする。 ⑷１次受付においてヘルプデスクで回答可能と判断した問い合わ

項目	内容
	せについて回答を検討し、利用者に対して回答する。 (5)ヘルプデスクでの問い合わせ対象は、次のとおりである。 ・　クライアント PC 及びプリンタ等の機器の故障 ・　業務システムの機能に関する事項 ・　ソフトウェア及び機器の操作方法 ・　その他、システム全般に係わる事項　等 ○問い合わせ内容の記録と分析、FAQ 掲載内容の抽出と更新 (1)受け付けたすべての問い合わせについて、利用者情報及び問い合わせ内容等をヘルプデスクシステムに登録する。 (2)利用者への回答完了後、回答内容等をヘルプデスクシステムに登録する。 (3)頻度の高い問い合わせ、回答内容を抽出し FAQ に掲載する。
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	―

6. 利用者満足度調査

項目	内容
役務内容の概要	システム利用者に対する満足度調査の実施と報告
想定されるインプット （発注者側で用意）	調査アンケート
成果物 （受注者側で用意）	利用者満足度調査報告書
仕様書に記載すべきポイント	**【1. 基本的に記載すべき要求要件】** ・満足度調査の実施 ・調査アンケートの対象および方法 ・調査結果の報告 ・担当官と協議の上、ヘルプデスク業務の運用改善の実施
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○システム利用者に対する満足度調査の実施と調査結果の報告、運用改善の実施 受注者は、利用者満足度調査を実施し報告すること。また、この調査結果を踏まえ、○○省専任部門と受託者による協議の上、ヘルプデスク業務の運用の改善を実施すること。
案件・情報システムの特性等による留意点	—
セキュリティに関する留意点	—

7．ヘルプデスク運用会議

項目	内容
役務内容の概要	定例会議体などでヘルプデスク業務の運用報告を行う。必要に応じて課題と解決方法に関する検討を行う。（月次、週次、年次、緊急報告会　等） 会議に係る各種報告書を作成・提出する。
想定されるインプット （発注者側で用意）	・納品物一覧 ・実施スケジュール（案）［運用会議開催日程（案）］
成果物 （受注者側で用意）	・月次報告書 ・議事録
仕様書に記載すべきポイント	文書にて報告、提出を求めるドキュメント類を抽出し、提出する旨を記載する。また、各タイミングでレビュー・承認プロセスを行う。 **【1.　基本的に記載すべき要求要件】** ・報告書の作成とレビュー ・報告と承認のプロセスが必要な会議体の概要や開催頻度、参加者
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○報告書の作成とレビュー 受託者は、ヘルプデスク業務作業の稼働状況等について、以降に示す会議において、○○省専任部門へ報告することとする。また、受託者内において、稼働状況等を確認するための会議等を随時実施し、状況把握に努め報告準備すること。 なお、本業務に支障をきたすような緊急又は重大な問題が発生した場合には、定例会議を待たず速やかに○○省専任部門へ報告し、対応を協議すること。 ○報告と承認のプロセスが必要な会議体の概要や開催頻度、参加者 受託者は、運用センター全体で実施する以降に示す会議に出席すること。 なお、運用報告会議及び年間評価会議については、○○省専任部門が指定する場所（都内を予定）で開催する。個別調整会議の開催場所については、都度、関係者と調整を行うこと。また、会議体の詳細については、受託後に、○○省専任部門と協議の上、決定すること。 ①導入状況報告会議 ヘルプデスク導入期間中において、ヘルプデスク業務環境整備、要員の教育の進捗状況等について報告を行う。

項目	内容
	開催頻度　隔週 出席者 ・〇〇システム事務局 ・統括責任者 ・ヘルプデスク担当業者 ②運用報告会議 〇〇システム事務局に対して稼働状況やサービスレベル指標の報告を行う。 開催頻度　月に１回 出席者 ・〇〇システム事務局 ・統括責任者 ・運用サービス担当業者 ・ヘルプデスク担当業者 ・アプリケーション保守サービス担当業者 ・ハードウェア保守サービス担当業者 ③年間評価会議 年間を通じたサービスの実績や結果対応の状況などを報告するとともに、サービスレベル指標の妥当性を評価する。 開催頻度　年に１回 出席者 ・〇〇システム事務局 ・統括責任者 ・運用サービス担当業者 ・ヘルプデスク担当業者 ・アプリケーション保守サービス担当業者 ・ハードウェア保守サービス担当業者 ④個別調整会議 個別の調整が必要となった場合に、必要に応じて開催する。 開催頻度　随時 出席者　随時調整する
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	―

6.5.3.納入成果物と提出のタイミング

納入成果物とタイミングをまとめると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	納入成果物	納入期限
1.運用計画の策定	実施計画書 ヘルプデスク環境構築図 導入計画書 運用計画書、運用実施要領	契約締結後2週間以内 契約締結後2週間以内 契約締結後1ヶ月以内 サービス開始まで
2.運用のための引継ぎ業務	後任事業者への引継計画書 後任事業者への引継ぎ資料	引継ぎ開始1ヶ月前
3.作業環境の整備	ヘルプデスク業務教育資材 ヘルプデスク業務マニュアル ヘルプデスク用電話回線 ヘルプデスク用電話回線の敷設図 音声応答サーバ用電話回線 音声応答サーバ用電話回線の敷設図	サービス開始まで
4.サービスレベル管理	サービスレベル合意書(SLA) サービスレベル報告書	サービス開始まで 月次
5.ヘルプデスク業務運用	FAQ情報 稼動状況報告書 問い合わせ･対応履歴情報	月次 問い合わせ･対応履歴情報は、業務終了時
6.利用者満足度調査	利用者満足度調査報告書	指定する期日まで
7.ヘルプデスク運用会議	月次報告書 完了報告書 議事録	月次 指定する期日まで

6.5.4.想定されるインプット

既存の仕様書の事例の中から、受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングをまとめると、下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	インプット	インプットを提示するタイミング
1. 運用計画の策定	導入予定及び利用者の概算人数 役割分担 全体スケジュール 体制図 運用体制	入札公示時に調達仕様書・付属資料に記載する
2. 運用のための引継ぎ業務	前任事業者（新規システムの構築の場合は、システム構築事業者）からの引継計画書 前任業者からの引継ぎ資料、業務内容、運用作業、セキュリティ等に係る研修	入札公示時に調達仕様書・付属資料に記載する
3. 作業環境の整備	回線の敷設における制約事項 ヘルプデスク運用マニュアル変更に必要となる、制度改正やシステム改修の詳細	入札公示時に調達仕様書・付属資料に記載する
4. サービスレベル管理	サービスレベル項目／定義書	入札公示時に調達仕様書・付属資料に記載する
5. ヘルプデスク業務運用	―	―
6. 利用者満足度調査	―	―
7. ヘルプデスク運用会議	納品物一覧	入札公示時に調達仕様書・付属資料に記載する

サービスレベル項目の例

項番	サービスレベル項目	規定内容	単位
1	ヘルプデスク サービス提供時間帯(障害対応)	障害対応時の問合せ受付業務を実施する時間帯	時間帯
2	ヘルプデスク サービス提供時間帯(一般問合せ)	一般問合せ時の問合せ受付業務を実施する時間帯	
3	平均回答時間	受付から問題解決の回答までに要する時間	時間
4	1 次回答時間	障害受付から、オペレータが 1 次回答をするまでの時間	時間
5	ヘルプデスク 問い合わせ数	1日の平均的な問合せ件数	件/日
6	ヘルプデスク 電話ビジー率 電話放棄率	電話ビジー率 電話がつながらなかった比率 電話放棄率 電話を取ることができなかった比率	%
7	ヘルプデスク 問題解決率(時間)	取り決めをした問題解決(クローズ)までの時間で解決した比率	%
8	ヘルプデスクエスカレーション時間･回数	エスカレーションまでに要する時間と比率･回数	%･回
9	ヘルプデスク バックログ率	1日の終了時点で未解決の問題の比率	%
10	ヘルプデスク再コール率	一度問題解決とした問題で、再度問合せがある比率	%
11	サービスデスク 情報システム関連の利用申請のサービス時間帯	イントラ/インターネットの利用申請(共通ID管理システム(LDAP)の利用申請)や、メールの利用申請、モバイルの利用申請など	時間帯
12	サービスデスク 申請処理日	各種の利用申請を実施するまでの時間(日数)	日
13	報告	定例報告	項目
14		受付状況を随時 Web で確認できるようにし、業務システムの変更などがあった場合の問合せ状況などを把握できるようにする。	項目

6.5.5.役割分担

ヘルプデスク運用事業者と府省庁、その他業務の調達事業者との役割分担について、一例をここでは紹介する。

分離・分割調達では分離発注の範囲、府省庁における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。
調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、提示することが必要である。

役割分担の例

○：主担当、△：支援、助言

作業項目	主管課	ｼｽﾃﾑ構築事業者	HW 保守事業者	SW 保守事業者	AP 保守事業者	運用事業者	iDC 事業者	ﾍﾙﾌﾟﾃﾞｽｸ事業者
運用計画の策定	○	△	－	－	－	△	△	○
運用のための引継ぎ業務	○	○	△	△	△	△	△	○
作業環境の整備	△	－	－	－	－	△	△	○
サービスレベル管理	○	－	－	－	－	△	－	○
ヘルプデスク業務運用	△	－	△	△	△	△	△	○
利用者満足度調査	○	－	－	－	－	－	－	○
ヘルプデスク運用会議（報告）	○	－	△	△	△	○	△	○
ヘルプデスク運用会議（評価）	○	－	○	○	○	○	○	○

※　システム構築事業者は、新規システムの構築を行い運用のための引継ぎを行う場合

6.6.保守

保守作業は情報システム稼働後に顕在化したエラーの修正、システムに対する軽微な機能変更要求に対処する役務である。

本工程の役務は、障害や問題の発生を事前に予防するために実施する定期保守（定期点検）、問題・障害発生時に実施する緊急保守、システム利用者、主管課等に対するサポートなどである。

これら本工程の役務詳細は前工程である「設計・開発」フェーズの保守設計で策定されるので、保守設計の成果物が本工程のインプットとなる。

保守で実施される４つの詳細役務を表 6.6.1 に示す。

役務詳細分類	定義
6.6.1. ハードウェア保守	ハードウェア（サーバ、ストレージ、共通 PC、オフィスプリンタ、ネットワーク機器：ルータ・スイッチなど）に対する保守（ハードウェアの組込みソフトウェアを含む）
6.6.2. ソフトウェア保守	商用ＯＳ、商用ミドルウェア、商用アプリケーションパッケージソフトウェアに対する保守　（ＯＳＳのＯＳ・ミドルウェア・業務ソフトウェアは含まない）
6.6.3. アプリケーション保守	商用ＯＳ・商用パッケージソフトウェア以外の業務アプリケーションソフトウェアに対する保守（ＯＳＳのＯＳ・ミドルウェア・業務ソフトウェアも含む）
6.6.4. システム基盤保守	技術参照モデルの「第５章技術ドメイン解説」のうち、「EIP」「公開 Web サーバ」「グループウェア、ファイルサーバ、メールサーバ」「統合アカウント管理・認証・認可(アクセス制御)」「統合ディレクトリ」「WAN・省内 LAN、DNS/DHCP/Proxy、リモートアクセス」「ネットワーク回線」などに関する保守

表 6.6.1　保守の役務詳細分類と定義

6.6.1.ハードウェア保守

6.6.1.1. 調達分野の定義

ハードウェア保守は、ハードウェア（サーバ、PC、プリンタ、ストレージ、オフィスプリンタ、ネットワーク機器：ルータ・スイッチなど）に対する保守役務である。

ハードウェア保守に係る役務調達は、物品（機器提供）、機器の据付・調整、環境の整備等も同じ契約の中で調達する場合があるが、本項の記載ではハードウェア保守に関わる役務についてのみ記載している。

図 6.6.1 -1 役務調達の分類における対応箇所

6.6.1.2. 仕様書に記載すべき役務内容

6.6.1.2.1.代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応するSLCP-2007のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCPのアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務の概要	共通フレーム2007のアクティビティ	調達基本指針に対応する仕様書の章･節（及びそのタイトル）
1.ハードウェア保守計画の策定	ハードウェア保守計画書（保守作業計画、作業体制等）の策定	1.8.1.2 計画及び手続きの作成	11章(2)　ハードウェア保守要件 （および、要約を　2章(5)　作業内容・納入成果物　へ記載）
2.サービスレベル管理	役務サービスの品質（レベル）を確保する必要がある場合、サービスレベル合意書（SLA）の締結、サービスレベル管理指標に関する作業状況の記録	ー	
3.定期保守･定期点検	保守要領等に基づく、年1回以上の予防点検の実施、消耗部品等の交換	1.8.2.1 問題報告又は修正依頼の分析	
4.障害対応	ハードウェア障害時の現地対応（オンサイトサポート）	1.8.3.1 分析と修正部分の決定 1.8.3.2 修正の実施	
5.バージョンアップの支援	ファームウェア等のリリース情報提供、バージョンアップ作業	1.8.3.2 修正の実施	
6.技術支援	主管課、運用支援事業者等からの依頼に基づく、技術支援	1.7.6.2 利用者支援 1.8.2.2 問題の再現又は検証	

6.6.1.2.2.各役務内容に関する説明及び仕様書上の記載例

1．ハードウェア保守計画の策定

項目	内容
役務内容の概要	ハードウェア保守計画書（保守作業計画、平常時・緊急時の連絡先を記した体制表等を含む）を策定する。
想定されるインプット （発注者側で用意）	・保守要領 ・保守手順書 ・保守計画（案） ・サービスレベル合意書（SLA）（案） ・役割分担表（当該システムの関連事業者、発注者）
成果物 （受注者側で用意）	・ハードウェア保守計画書 （工程表、通常・障害時連絡体制表、保守体制表　等を含む）
仕様書に記載すべきポイント	保守計画策定に関する要求事項を記載する。 **【1.基本的に記載すべき要求要件】** ・保守対応時間 ・計画書に含めるべき内容（工程表、障害時連絡体制表、保守拠点一覧などを記載） ・計画書の提出期限 ・保守作業における役割分担（役割分担の記載例は 6.6.1.5 を参照） **【2.案件の種類・特性によって追記すべき要求要件】** ・SLA の順守
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①保守業務時間は、閉庁日を除く平日 9:00～18:00（休日・祝日を除く）、オンサイト保守とする。ただし、ハードウェア障害が業務に重大な影響を及ぼす場合、システム停止を伴う保守点検等は上記時間に関わらず対応すること。 ②受注者は、「本調達仕様書」及び別途提示する「保守設計書」、「保守手順書」等に基づき、定期点検、ハードウェアメンテナンス作業などの保守計画、平常時・緊急時の保守実施体制表を作成し、受注後 14 日以内に主管課に提出して承認を得ること。 ③受注者は保守作業計画策定にあたり、システム（サービス）停止の回避等、業務に支障をきたさないよう十分に配慮すること。　業務への影響がある保守作業については実施日を主管課と調整の上、休日等の対応にも応じること。また、運用・保守関係事業者と定期点検・定期保守の作業スケジュールを調整して、システム停止時間、

項目	内容
	保守時間が最小化されるように配慮して日程や時間割を行い、保守計画の策定を行うこと。 ④受注者は、保守対象機器の障害発生時及び主管課の求めに対して、標準保守対応時間に迅速な保守対応ができる体制を構築し、主管課の承認を得ること。なお、保守要員は、保守対象機器に関する十分な知識、経験等を有する技術者であること。 【2.案件の種類・特性によって追記すべき要求要件】 ⑤受注者は調達仕様書及び受注者が調達時に示した提案書に基づき、サービスレベル合意書（SLA）を締結すること。また、受注者はサービスレベル管理指標を遵守するために必要な予防保守、障害対応のための保守体制等に配慮した保守計画を立案すること。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	－

2．サービスレベル管理

項目	内容
役務内容の概要	ハードウェア保守に伴う役務サービスの品質（レベル）を確保する必要がある場合、サービスレベル指標及び目標値を設定し、サービスレベルの管理を行う。
想定されるインプット（発注者側で用意）	・サービスレベル合意書（SLA）（案） （サービスレベル管理指標を含む）
成果物（受注者側で用意）	・サービスレベル合意書（SLA） （サービスレベル管理指標を含む） ・サービスレベル管理計画書 ・サービスレベル報告書
仕様書に記載すべきポイント	サービスレベル管理指標及びサービスレベル合意書（SLA）案を具体的に明示する。 これらサービスレベル管理指標、サービスレベル合意書（SLA）案は調達者側の考える案であり、両者で協議後に形式に合意文書（契約書）を締結すること、協議により変更をする余地がある旨を記載する。 また、SLA 遵守を特に厳しく求める場合は、定期的なサービス指標実績レビューの実施や、SLA を遵守できなかった場合に求める改善プロセスやペナルティについて記載する。 なお、サービスレベル管理は必須要件でないので、調達案件に SLA の適用が必要か否かを十分に検討を行うこと。 **【2.案件の種類・特性によって追記すべき要求要件】** ・サービスレベル管理指標（案） ・サービスレベル合意書締結前の協議の実施 ・支払金額やペナルティに関する考え方 ・サービスレベル管理指標の実績測定、及び SLA 達成度に対する定期的なレビュー実施 ・SLA が遵守できなかった場合の対応要件（無償対応や改善のための取り組み）

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>仕様書記載上の例/説明</td><td>仕様書に記載する場合の例

【1.基本的に記載すべき要求要件】
①本調達では受注者の提供する保守の高い品質が維持されていることを検証するため、受注者と協議のうえ、サービスレベル合意書（Service Level Agreement）を締結する。受注者は、本仕様書が示すサービスレベル管理指標を基にサービスレベルの維持・向上に資するサービスレベル合意書案を策定し、提案書にて提示すること。

<table>
<tr><td>No</td><td>サービスレベル管理指標</td><td>説明</td><td>指標値</td></tr>
<tr><td>1</td><td>平均故障復旧時間（MTTR）</td><td>平均故障復旧時間は、サービス稼働時間中において、機器に故障が発生した時刻から故障が復旧した時刻までに要した時間の 1 ヶ月間における平均値である
故障が発生した時刻は、障害を検知、又は通報等により認識した時刻とする
障害復旧は、機器の故障原因を排除し、正常に稼働することを確認し、利用者が使用可能な状態であることをいう</td><td>6 時間以内</td></tr>
</table>
②受注者は、主管課と締結したサービスレベル合意書に基づき、サービスレベル管理指標毎の実施状況を毎月計測し、３か月毎に開催するサービスレベル報告会において、達成状況の報告を行うこと。

【2.案件の種類・特性によって追記すべき要求要件】
③受注者からのサービスレベル達成状況報告を基に、受注者と主管課は協議を行い、当該期間におけるサービスレベル合意書の達成度合いを判定する。委託金額の支払はサービスレベル合意書の達成度に合わせて決定する。未達成 SLA 項目が 90%未満の場合には受注者</td></tr>
</table>

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td></td><td>の負担で改善提案を行い、主管課の承認を得たうえで、対策を実施すること。
<table>
<tr><th>達成度合い</th><th>支払の割合</th><th>条件</th></tr>
<tr><td>A</td><td>100%(満額)</td><td>全 SLA 項目で指定条件達成</td></tr>
<tr><td>B</td><td>97%</td><td>指定条件を達成できない SLA 項目が SLA 項目数全体のうち 5%未満</td></tr>
<tr><td>C</td><td>94%</td><td>指定条件を達成できない SLA 項目が SLA 項目数全体のうち 5%以上 10%未満</td></tr>
<tr><td>D</td><td>90%</td><td>指定条件を達成できない SLA 項目が SLA 項目数全体のうち 10%以上</td></tr>
</table></td></tr>
<tr><td>案件・情報システムの特性等による留意点</td><td>サービスレベル管理は必須の要件でなく、保守役務の品質を重視する場合に設定する要件である。
サービスレベル指標や目標の設定、過剰な要件追加は、委託費用が高額となる可能性があるので注意が必要である。</td></tr>
<tr><td>セキュリティに関する留意点</td><td>－</td></tr>
</table>

3．定期保守･定期点検

項目	内容
役務内容の概要	保守要領等に基づき、年 1 回以上の定期点検を実施し、消耗部品等の交換や機器調整等を実施する。
想定されるインプット （発注者側で用意）	保守要領 保守手順書
成果物 （受注者側で用意）	・定期保守報告書
仕様書に記載すべきポイント	【１．基本的に記載すべき要求要件】 ・定期保守の実施回数、頻度 ・定期保守の作業内容（清掃、点検、テストプログラムによる診断、作業完了後の動作確認） ・定期保守の対象機器 ・作業時間の制約 ・保守報告書の作成と、定期保守完了の報告 ・故障発見時の対応
仕様書記載上の例/説明	仕様書に記載する場合の例 【１．基本的に記載すべき要求要件】 ①受注者は、「保守計画書」、「保守要領」、「保守手順書」等に基づき、年１回保守点検を行うこと。 ②受注者は、当該システムの停止に伴う業務への影響に十分配慮し、定期点検の詳細計画書の策定を行うこと。定期点検の実施に伴い、システムの停止等が発生する場合には予め主管課と協議し、承認を得ること。 ③受注者は、「保守計画書」に基づいて、保守作業を実施した都度、「保守実施報告書」を作成し、作業結果について主管課の承認を得ること。 ④受注者は、保守点検の結果、発見された故障・問題に対する対応計画を立案し、主管課の承認を得ること。ただし、定期点検にあわせて対応した場合は「保守実施報告書」の提出により代替してもよい。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	

4. 障害対応

項目	内容
役務内容の概要	ハードウェア障害の受付を行い、障害復旧のための現地対応（オンサイトサポート）を行う。
想定されるインプット （発注者側で用意）	・保守要領 ・保守手順書 ・障害切り分け手順書
成果物 （受注者側で用意）	・障害報告書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・障害発生時の対応サービス提供日・時間の定義 ・故障修理作業報告書作成 **【2.案件の種類・特性によって追記すべき要求要件】** ・物理破壊などによる、ハードディスクの廃棄交換時のデータの完全消去 ・センドバック保守対象の機器についてはハードウェア保守事業者事前に代替機を準備し、障害発生時に速やかに交換作業を行うこと。
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①受注者は保守業務時間内に受信した保守対象機器の障害発生通報、又は主管課からの対応依頼に応じて、保守要員の派遣を行うこと。ただし、緊急の際は主管課と協議の上で保守業務時間外でも個別対応を行うこと。 ②受注者は、交換部品等の調達・交換・補修等を迅速に行い、保守対象機器の早期復旧を図ること。 ③ハードディスクの交換等により再インストールやデータリカバリが必要な場合は主管課を通じて、アプリケーション保守業者、システム保守業者に作業依頼を行うこと。 【2.案件の種類・特性によって追記すべき要求要件】 ④ハードディスク及びテープメディア等の外部記録媒体が故障し、ハードディスク及びテープメディア等の外部記録媒体を機器設置場所から持ち出すときには外部記録媒体に保存されているデータを完全に消去するか、物理的に破壊し、主管課の承認を得た上で搬出すること ⑤保守対象機器がセンドバック方式のみとなっている場合は、予め障害発生時の代替機を受注者が準備し、当該機器の障害発生時に速やかな交換作業を実施すること。

項目	内容
案件・情報システムの特性等による留意点	障害対応は、運用事業者、ソフトウェア保守事業者、アプリケーション保守事業者、システム基盤保守事業者、関連システムの関係者等との共同作業となるため、関係する事業者との役割分担、各事業者の責任範囲を明確に示す必要がある。
セキュリティに関する留意点	―

5．バージョンアップの支援

項目	内容
役務内容の概要	ファームウェア等のリリース情報を入手し、主管課に提供する。また、主管課と協議の上、ファームウェア等のバージョンアップを行う。
想定されるインプット（発注者側で用意）	・保守要領 ・保守手順書
成果物（受注者側で用意）	・作業報告書
仕様書に記載すべきポイント	【1.　基本的に記載すべき要求要件】 ・パッチ・アップデートに対する報告と提供 ・パッチ・アップデートのリリースから報告までの対応時間 ・提出ファイルの形式等 ・ファームウェア更新に伴う環境設定等の変更作業
仕様書上の記載例	仕様書に記載する場合の例 【1.　基本的に記載すべき要求要件】 ①受注者は保守対象機器のファームウェア等に関するアップデート情報を当該機器の製造者・代理店等の供給者等より入手し、アップデート情報公表後７日以内に主管課に報告すること。 ②受注者は、入手したアップデート情報のうち、当該機器への適用が必要と判断したファームウェアについては主管課の承認を得たうえで、府省の承認から１ヶ月以内に当該機器への適用を行うこと。 ③ファームウェア等のバージョンアップ作業は主管課の承認を得たうえで、システム稼働に影響を与えないよう、作業日程・時間に十分配慮して実施すること。なお、ファームウェアバージョンアップに伴い、設定変更が必要となる場合には作業時に設定の変更も行うこと。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	ファームウェアの更新、設定変更等 ＢＩＯＳなどセキュリティやハードウェアの安定性に関係するファームウェアは常に最新の情報を入手し、必要に応じた更新作業の実施をハードウェア保守事業者に求めること。

6. 技術支援

項目	内容
役務内容の概要	主管課および運用事業者から依頼に基づき、技術支援を実施する。
想定されるインプット （発注者側で用意）	保守手順書 保守要領 問い合わせ元の所属・人数（想定）
成果物 （受注者側で用意）	・技術支援実施報告書
仕様書に記載すべきポイント	【1.基本的に記載すべき要求要件】 支援依頼の受付時間 技術的な問い合わせへの対応 問題切り分けに対する支援 【2.案件の種類・特性によって追記すべき要求要件】 問い合わせへの回答期限 主管課、運用支援業者への支援作業実施結果報告
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 受注者は主管課、運用事業者からの問い合わせに対して、迅速に回答・助言を行うこと。 受注者は主管課、運用事業者からのエスカレーションに対して、保守要員を現地に派遣し、主管課、運用事業者、他の保守事業者等の関連者に協力して問題解決の支援を実施すること。 受注者は、必要に応じてハードウェアログの解析、ハードウェア設定情報等の確認・提供等を実施し、問題解決にあたること。また、問題がハードウェアに起因することが判明した場合には速やかに復旧作業を実施すること。 問い合わせの受付時間は、行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項に掲げる日をいう。）を除く日の原則 9:00～18:00 とする。 受注者は、問題解決支援作業や復旧作業等の終了後、速やかに作業結果を主管課に報告を行うこと。 【2.案件の種類・特性によって追記すべき要求要件】 受注者は、問い合わせ受付後 2 日以内（行政機関の休日（「行政機関の休日に関する法律」（昭和 63 年法律第 91 号）第 1 条第 1 項）を除く）に回答や分析結果の報告を行うこと。回答期限までに回答等ができない場合は問い合わせ元に対して回答期限までに進捗状況と回答予定日を連絡すること。

項目	内容
	受注者は、支援作業の完了後、速やかに作業報告を主管課及び運用支援業者に実施すること。
案件・情報システムの特性等による留意点	統合ヘルプデスクなど、統括的な問い合わせ受付窓口が設置される場合には、これらの窓口からのエスカレーションを可能とする仕様を追加すること。
セキュリティに関する留意点	－

6.6.1.3.納入成果物と提出のタイミング

ハードウェア保守業務に対する納入成果物と納入期限の例は以下の通りである。各成果物の正式名称、納入期限は実態に即して記載をする必要がある。

役務作業	納入成果物	納入期限例
1. ハードウェア保守計画の策定	ハードウェア保守計画書 保守要領・保守手順書（改定版）	契約締結後 14 営業日以内
2. サービスレベル管理	サービスレベル合意書 サービスレベル管理計画書	契約締結後 14 営業日以内
	サービスレベル管理結果報告書	サービスレベル計測期間毎、指定する期日
3. 定期保守・定期点検	定期保守報告書	作業完了後、7 営業日以内
4. 障害対応	障害報告書	作業完了後、7 営業日以内
5. バージョンアップの支援	作業報告書	作業完了後、7 営業日以内
6. 技術支援	問い合わせ管理表	指定する期日
	作業計画書（支援依頼分）	作業実施 14 営業日以前
	支援作業実施報告書	作業完了後、7 営業日以内

6.6.1.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプット、インプットのタイミングは下記の通りである。各インプットの正式名称、納入期限は実態に即して記載をする必要がある。

役務作業	インプット	インプットを提示するタイミング
1.ハードウェア保守計画の策定	保守計画（案） サービスレベル項目／定義書 サービスレベル合意書 役割分担（SOW）	調達仕様書に記載、又は別添資料として添付する
	保守要領 保守手順書	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
2. サービスレベル管理	サービスレベル項目／定義書 サービスレベル合意書	調達仕様書に記載、又は別添資料として添付する
3.定期保守・定期点検	保守要領 保守手順書	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
4.障害対応	保守要領 保守手順書	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
5.バージョンアップの支援	保守要領 保守手順書	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
6.技術支援	保守要領 保守手順書	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。

6.6.1.5.役割分担

ハードウェア保守事業者と府省、その他業務の調達事業者との役割分担の例を以下に示す。

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表を作成することが必要である。

○：主担当、△：支援、助言

作業項目	主管課	HW 保守事業者	SW 保守事業者	AP 保守事業者	運用事業者	iDC 事業者	ヘルプデスク事業者
ハードウェア、パッケージソフトウェア、ネットワーク等の運用保守計画の企画、調達	○	△		△	△	△	－
ハードウェアのオンサイトサポート	－	○	-	－	△	△	－
パッケージソフトウェアのパッチ提供、オフサイトサポートの実施	－	－	○	－	△	△	－
ネットワークのオンサイトサポート	－	－	－	－	○	△	－
システムの日常オペレーション	－	－	－	－	○	△	－
システム、ネットワーク監視	－	－	－	－	○	△	－
セキュリティ監視	－	－	－	－	○	△	－
利用者からの問い合わせ対応	○	－	－	－	－	－	○
主管課からの問い合わせ、統合ヘルプデスクからエスカレーション対応	－	○	○	○	○	○	○
問題発生時の一次切り分け	△	△	△	△	○	△	－
問題発生時の二次対応（ハードウェア障害）	△	○	△	△	△	△	－
問題発生時の二次対応（ソフトウェア／アプリケーションソフトウェア障害）	△	△	△	○	△	△	－
問題発生時の二次対応（iDC 設備障害）	△	△	△	△	△	○	－
障害発生時のシステムリカバリ処理	△	△	－	○	○	－	－
アプリケーションソフトウェアの保守	△	－	－	○	－	－	－
運用管理情報の収集、分析、報告、提言	△	△	－	△	○	△	－
消耗品の管理	－	－	－	－	○	－	－

表 6.6.1.5.1 運用・保守事業者の役割分担（例）

6.6.2.ソフトウェア保守

6.6.2.1.調達分野の定義

ソフトウェア保守は商用OS、ミドルウェア、アプリケーションソフトウェア等の製品に対する保守役務で、新規に開発されたソフトウェアやオープンソフトウェア（OSS）など、商用製品以外のソフトウェアは本役務に含まない。

ソフトウェア保守はハードウェア保守と同時に調達されることが多いが、本項ではソフトウェア保守に関する役務についてのみ記載している。

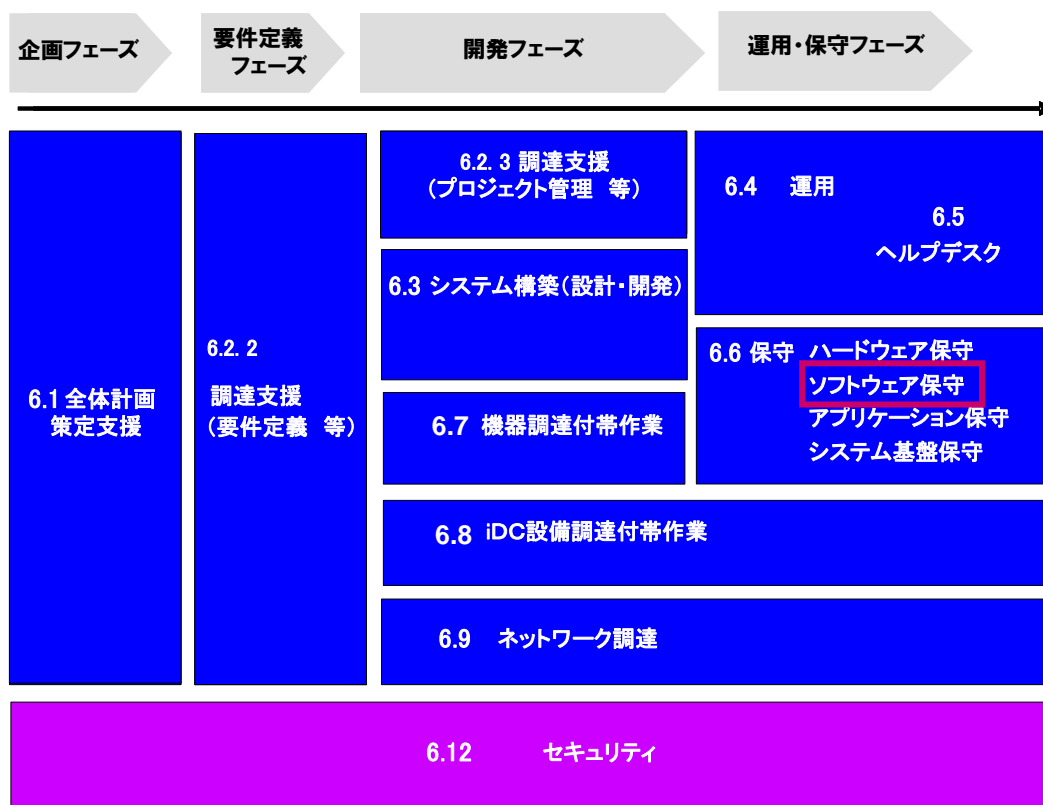



図 6. 6.2.−1 役務調達の分類における対応箇所

6.6.2.2.仕様書に記載すべき役務内容

6.6.2.2.1.代表的な役務作業の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応するSLCP-2007のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCPのアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務の概要	共通フレーム2007のアクティビティ	調達基本指針に対応する仕様書の章・節
1. ソフトウェア保守計画の策定	各製品の保守サービス詳細、平常時・緊急時の連絡先等を記したソフトウェア保守計画の策定	1.8.1.2 計画及び手続きの作成	11章 (1) ソフトウェア保守要件 （および、要約を 2章(5) 作業内容・納入成果物 へ記載）
2. 修正（パッチ）ファイル、バージョンアッププログラムの提供	修正（パッチ）ファイル等のリリース情報及び修正ファイルの提供、	1.8.1.2 計画及び手続きの作成 1.8.3.1 分析と修正部分の決定 1.8.3.3 購入パッケージの修正実施	
3. 技術支援	保守対象ソフトウェアに関する技術支援（オフサイトサポート）の提供	1.7.6.2 利用者支援	

6.6.2.2.2.各役務内容に関する説明及び仕様書上の記載例

1．ソフトウェア保守計画の策定

項目	内容
役務内容の概要	ソフトウェア保守計画（各製品の保守サービス詳細、平常時・緊急時の体制等）を策定し、主管課の承認を得る。
想定されるインプット （発注者側で用意）	・保守要領 ・保守対象ソフトウェア一覧
成果物 （受注者側で用意）	・保守計画書 （工程表、通常・障害時連絡体制表、保守体制表　等を含む）
仕様書に記載すべきポイント	保守計画策定に関する要求事項を記載する。 【1.基本的に記載すべき要求要件】 ・受注者に求める体制と成果物 ・サポートの提供時間（問い合わせ窓口の開設時間）
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①受注者は、「本調達仕様書」及び別途提示する「保守設計書」、「保守手順書」等に基づき、保守計画を作成・納入し、主管課の承認を得ること。 ②受注者は、保守対象ソフトウェアの不具合発生時及び主管課の求めに対して、標準保守対応時間の問い合わせに迅速な対応ができる窓口を設定し、主管課の承認を得ること。なお、保守要員は、保守対象ソフトウェアに関する十分な知識、経験等を有する技術者であること。 ③受注者は、保守対象ソフトウェアの不具合発生時及び主管課の求めに対して、標準保守対応時間の問い合わせに迅速な対応ができる窓口を設定し、主管課の承認を得ること。なお、保守要員は、保守対象ソフトウェアに関する十分な知識、経験等を有する技術者であること。
案件・情報システムの特性等による留意点	ソフトウェア保守は他の保守と異なり、オンサイト作業が提供されず、オフサイトサポートのみが提供されるという特徴がある。 基幹システムにおけるソフトウェア保守業務では、問い合わせ可能時間を延長することを考慮することが望ましい。
セキュリティに関する留意点	－

2．修正(パッチ)ファイル、バージョンアッププログラムの提供

項目	内容
役務内容の概要	保守対象ソフトウェアの修正（パッチ）ファイル、バージョンアッププログラムの提供、及び同プログラムなどのリリース情報を提供する。
想定されるインプット（発注者側で用意）	・保守対象ソフトウェア一覧
成果物（受注者側で用意）	・保守状況報告書
仕様書に記載すべきポイント	【１．基本的に記載すべき要求要件】 修正プログラム、バージョンアップ情報を速やかに提供 必要に応じて、ソフトウェア著作権者等と保守再委託契約を締結し、調達者に修正（パッチ）ファイルやバージョンアッププログラムの適用権が与えられるようにすること。
仕様書上の記載例	仕様書に記載する場合の例 ①受注者は、保守対象ソフトウェア製品の機能強化に対応するバージョンアッププログラム、不具合修正に対応するリビジョンアッププログラム等がリリースされた場合、速やかに主管課に通知すること。また、保守期間中にリリースされたバージョンアップ・リビジョンアッププログラム等に関するライセンス（使用権）の提供を行うこと。 ②同プログラム及び利用権の提供にあたり、必要がある場合は受注者の責において、当該ソフトウェア製品のライセンス提供元等と契約や調整を行うこと。
案件・情報システムの特性等による留意点	メジャーバージョンアップ等のソフトウェアアップグレードは当該ソフトウェア製品の使用許諾契約（ライセンス規定）により権利行使ができない製品もある。
セキュリティに関する留意点	ソフトウェアのバグ、パッチ及びバージョンアップ等に関する情報は入手次第、アプリケーション保守事業者又はシステム基盤保守事業者に通知し、パッチ適用可否の事前評価をアプリケーション保守事業者、又はシステム基盤保守事業者に指示する必要がある。 早急なパッチ適用可否を判断するために、ソフトウェア保守事業者が提供するソフトウェアバージョンアップ等の情報提供先にアプリケーション保守事業者、システム基盤保守事業者を加える方法もある。

3. 技術支援

項目	内容
役務内容の概要	保守対象ソフトウェアに関する技術的な問い合わせへの対応
想定されるインプット （発注者側で用意）	・保守対象ソフトウェア一覧
成果物 （受注者側で用意）	・問い合わせ回答
仕様書に記載すべきポイント	【1．基本的に記載すべき要求要件】 ・ソフトウェア技術相談の窓口の開設
仕様書上の記載例	仕様書に記載する場合の例 ・ 保守対象ソフトウェアに関する問い合わせ窓口を設け、当該ソフトウェアに関するサポートを行うこと。
案件・情報システムの特性等による留意点	ソフトウェア保守は他の保守と異なり、オンサイト作業が提供されず、電話・メール・Ｗｅｂ等によるオフサイトサポートのみが提供されることが多い。 基幹システムにおけるソフトウェア保守業務では、問い合わせ可能時間を延長することを考慮することが望ましい。
セキュリティに関する留意点	－

6.6.2.3.納入成果物と提出のタイミング

ソフトウェア保守に対する納入成果物と納入期限は以下の通りである。

各成果物の正式名称、納入期限に関しては実態に即して記載をする必要がある。

役務作業	納入成果物	納入期限
1. 保守計画策定	保守計画書	契約締結後 2 週間以内
2. 修正（パッチ）ファイル、バージョンアッププログラムの提供	修正（パッチ）ファイル アップグレードプログラム	パッチ、アップデートプログラムリリース時
3. 技術支援	問い合わせ回答	問い合わせ実施時（随時）

6.6.2.4.想定されるインプット

受注者(もしくは提案者)に対して事前に提示すべきインプット、インプットのタイミングは下記の通りである。各インプットの正式名称、納入期限に関しては実態に即して記載をする必要がある。

役務作業	インプット	インプットを提示するタイミング
1. 保守計画策定	保守対象ソフトウェア一覧	入札公示時に調達仕様書に記載、又は別添資料として添付する
2. 修正（パッチ）ファイル、バージョンアッププログラムの提供	保守対象ソフトウェア一覧	入札公示時に調達仕様書に記載、又は別添資料として添付する
3. 技術支援	保守対象ソフトウェア一覧	入札公示時に調達仕様書に記載、又は別添資料として添付する

6.6.2.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表で提示することが必要である。

○：主担当、△：支援、助言

作業項目	主管課	HW 保守事業者	SW 保守事業者	AP 保守事業者	運用事業者	iDC 事業者	ヘルプデスク事業者
ハードウェア、パッケージソフトウェア、ネットワーク等の運用保守計画の企画、調達	○	△		△	△	△	－
ハードウェアのオンサイトサポート	－	○	-	－	△	△	－
パッケージソフトウェアのパッチ提供、オフサイトサポートの実施	－	－	○	－	△	△	－
ネットワークのオンサイトサポート	－	－	－	－	○	△	－
システムの日常オペレーション	－	－	－	－	○	△	－
システム、ネットワーク監視	－	－	－	－	○	△	－
セキュリティ監視	－	－	－	－	○	△	－
利用者からの問い合わせ対応	○	－	－	－	－	－	○
主管課からの問い合わせ、統合ヘルプデスクからエスカレーション対応	－	○	○	○	○	○	○
問題発生時の一次切り分け	△	△	△	△	○	△	－
問題発生時の二次対応（ハードウェア障害）	△	○	△	△	△	△	－
問題発生時の二次対応（ソフトウェア／アプリケーションソフトウェア障害）	△	△	△	○	△	△	－
問題発生時の二次対応（iDC 設備障害）	△	△	△	△	△	○	－
障害発生時のシステムリカバリ処理	△	△	－	○	○	－	－
アプリケーションソフトウェアの保守	△	－	－	○	－	－	－
運用管理情報の収集、分析、報告、提言	△	△	－	△	○	△	－
消耗品の管理	－	－	－	－	○	－	－

表 6.6.2.5.1 運用・保守事業者の役割分担（例）

6.6.3.アプリケーション保守

6.6.3.1.調達分野の定義

アプリケーション保守は、スクラッチ開発された業務アプリケーション、カスタマイズされたパッケージソフトウェア（カストマイズ部分、もしくはカストマイズ部分を含むパッケージソフトウェア全体）に対する保守業務である。

定型保守サービスが存在しない、もしくはディストリビュータ等による保守サービスが提供されていないOSS（OS・ミドルウェア・業務ソフトウェア）の保守も本項に含まれる。

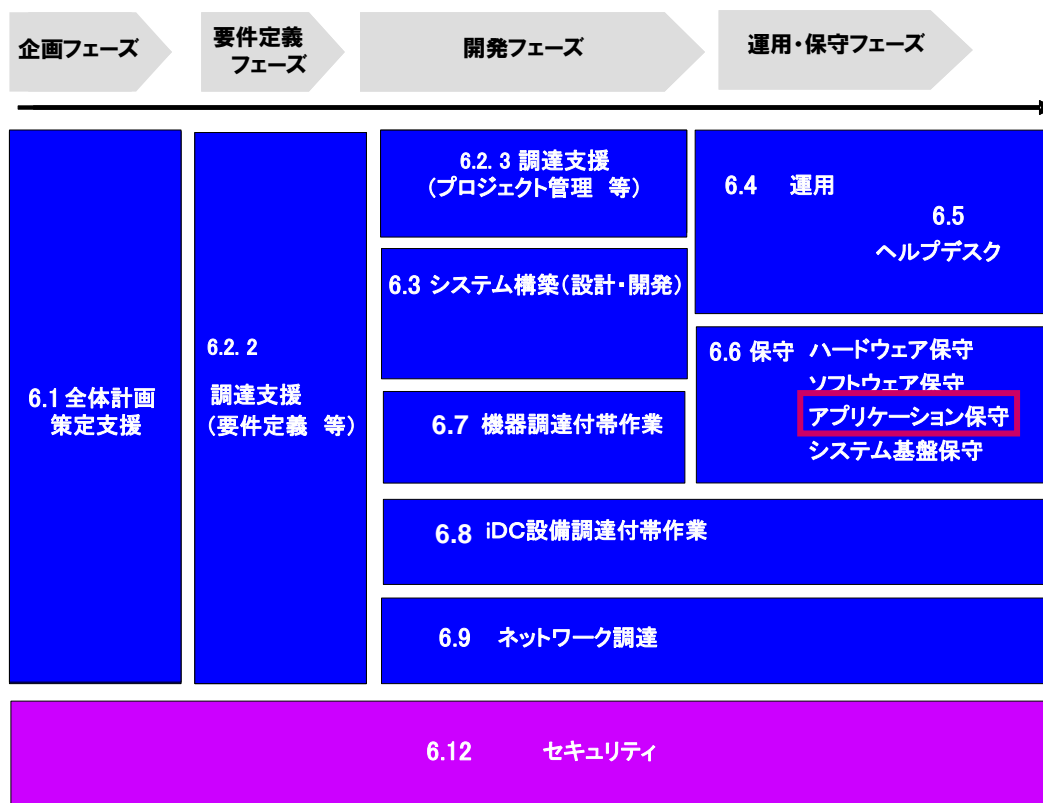



図　6.6.3-1　役務調達の分類における対応箇所

6.6.3.2.仕様書に記載すべき役務内容

6.6.3.2.1.代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務の概要	SLCP のアクティビティ	調達基本指針に対応する仕様書の章・節
1. 設計・開発事業者からの引継ぎ	設計・開発事業者からの引継ぎ		11 章(1) ソフトウェア保守要件 (および、要約を 2章(5) 作業内容・納入成果物 へ記載)
2. アプリケーション保守計画の策定	アプリケーション保守計画書（保守作業計画、平常時・緊急時の連絡先を記した体制表等を含む）の策定	1.8.1.2 計画及び手続きの作成	
3. サービスレベル管理	サービスレベル合意書（SLA）の締結、サービスレベル管理指標の順守状況の報告	―	
4. 障害対応	システム障害時の現地対応（オンサイトサポート）	1.8.2.1 問題報告又は修正依頼の分析 1.8.2.2 問題の再現又は検証	
5. プログラム修正	プログラムの部分改修・機能追加・バグフィックスのための開発、テスト、本番環境へのリリース、パッチ適用前のシステム影響分析、事前評価及び運用環境へのパッチ適用	1.6.6 ソフトウェア詳細設計 1.6.7 ソフトウェアコード作成及びテスト 1.6.8 ソフトウェア結合 1.8.2 問題把握及び修正分析 1.8.3 修正の実施 1.8.4 保守レビュー及び受入れ	
6. 技術支援	主管課および運用事業者からの依頼に基づく、技術支援の実施	1.8.3 修正の実施 1.8.4 保守レビュー及び受入れ	

6.6.3.2.2.各役務内容に関する説明及び仕様書上の記載例

1. 設計･開発事業者からの引継ぎ

項目	内容
役務内容の概要	設計・開発事業者からの引継ぎ
想定されるインプット （発注者側で用意）	【設計・開発事業者が作成した運用・保守関係の成果物】 ・ 保守計画書（案） ・ 保守設計書 ・ 保守手順書 ・ 保守ツール ・ 引継実施計画書
成果物 （受注者側で用意）	・ 引継実施報告書 ・ 保守計画書 ・ 保守体制表
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 引継実施報告書の作成 ・ 新システムの各本番稼動前、又は契約期間開始前に設計・開発事業者からの引継ぎを実施 ・ 保守設計書・保守手順等、引継元作成資料に関して疑義が生じた場合、引継元に対し、問い合わせや修正依頼を実施 ・ 保守手順作成資料に基づき、保守手順書を作成
仕様書記載上の例/説明	○設計・開発事業者等からの引継ぎ ▪ 受託者は契約完了後速やかに担当職員と協議し、平成○年○月末までに受託者の負担と責任において、保守対象のアプリケーションソフトウェアの内容及び保守業務等に関する引継ぎを設計開発事業者から受けること。 ▪ 受託者は保守に関する引継ぎを踏まえて、保守体制を整備し、保守計画書を作成すること。
案件・情報システムの特性等による留意点	－
セキュリティに関する留意点	－

2. アプリケーション保守計画の策定

項目	内容
役務内容の概要	アプリケーション保守計画書（保守作業計画、平常時・緊急時の連絡先を記した体制表等を含む）を策定する。
想定されるインプット （発注者側で用意）	・保守要領 ・保守手順書 ・サービスレベル管理指標（案） ・役割分担表（当該システムの関連事業者、発注者）
成果物 （受注者側で用意）	・実施計画書　等
仕様書に記載すべきポイント	保守計画策定に関する要求事項を記載する。 【1.基本的に記載すべき要求要件】 ・計画書に含めるべき作業内容（体制、進捗管理、品質管理、課題管理、変更管理、構成管理など）および受注者（アプリケーション保守事業者）における役割分担 【2.案件の種類・特性によって追記すべき要求要件】 ・＜複数年度契約の場合＞年度ごとの作業計画見直しに関する要件（例えば、SLA 等の要件の達成状況に応じた計画変更） ・＜特定のスキル・経験が求められるアプリケーション保守の場合＞作業者に求める資格・経験等　受注側の体制に求める要件　等
仕様書記載上の例/説明	仕様書に記載する場合の例 ①受注者は、「本調達仕様書」及び別途提示する「保守設計書」、「保守手順書」等に基づき、定期保守、アプリケーションメンテナンス作業などの保守計画を作成・納入し、主管課の承認を得ること。 ②保守作業計画はシステム（サービス）停止の回避等、業務に支障をきたさないよう十分に配慮した作業計画であること。業務への影響がある保守作業は実施日を調整の上、休日等の対応にも応じること。 ③受注者は、保守対象機器の障害発生時及び主管課の求めに対して、標準保守対応時間に迅速な保守対応ができる体制を構築し、主管課の承認を得ること。なお、保守要員は、保守対象アプリケーションソフトウェア及び当該アプリケーションシステムを含む保守対象システム全体に関する十分な知識、経験等を有する技術者であること。
案件・情報システムの特性等による留意点	対象システムもしくは類似した別のシステムの保守経験・設計開発経験など、特定の経験やスキル等が求められる案件については、特に求める担当者の要件について詳細に記載する必要がある。 保守作業や障害対応については、運用事業者、ハードウェア保守事

項目	内容
	業者、アプリケーション保守事業者、関連システムの関係者など、関係する事業者との役割分担、各事業者の責任範囲を明確に示す必要がある。 また、システム全体の構成管理に関しては、システム全体の構成管理を担う運用事業者の役割分担、責任範囲や構成管理の実施手順を示す必要がある。
セキュリティに関する留意点	―

3．サービスレベル管理

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>役務内容の概要</td><td>SLA の締結、サービスレベル管理指標に関する実績測定、SLA 未達成時の作業計画見直し等を実施する。
なお、サービスレベル管理は全ての案件に適用する必要はないので、調達時に SLA の適用が必要か否か、十分に検討を行うこと。</td></tr>
<tr><td>想定されるインプット
（発注者側で用意）</td><td>・サービスレベル管理指標（案）
・サービスレベル管理計画書</td></tr>
<tr><td>成果物
（受注者側で用意）</td><td>・サービスレベル報告書</td></tr>
<tr><td>仕様書に記載すべきポイント</td><td>【1.基本的に記載すべき要求要件】
なし。

【2.案件の種類・特性によって追記すべき要求要件】
保守業務実施の上で、受注者と発注者の間で締結する SLA についての要件を記載するとともに、サービスレベル管理指標に関して、両者で協議をする余地がある旨を記載する。
また、SLA 遵守を特に厳しく求める場合は、定期的なレビューの実施や、遵守できなかった場合の業務要件について記載する。
・府省と保守事業者でのサービスレベル管理指標に関する協議の実施
・SLA 項目の定義や注釈
・支払金額やペナルティに関する考え方
・定期的な SLA の遵守結果のレビュー実施
・SLA が遵守できなかった場合の対応要件（無償対応や改善のための取り組み）</td></tr>
<tr><td>仕様書記載上の例/説明</td><td>仕様書に記載する場合の例

【2.案件の種類・特性によって追記すべき要求要件】
①本調達では受注者の提供する保守の高い品質が維持されていることを検証するため、受注者と協議のうえ、サービスレベル合意書（Service Level Agreement）を締結し、受注者は、本仕様書が示すサービスレベル管理指標を基にサービスレベルの維持・向上に資するサービスレベル合意書案を策定し、提案書にて提示すること。

<table><tr><th>No</th><th>サービスレベル管理指標</th><th>説明</th></tr><tr><td>1</td><td>アプリケーションソ</td><td>アプリケーションの欠陥が発見</td></tr></table></td></tr>
</table>

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>フトウェアの修正</td><td>されてから1か月以内に対処が完了しているか。</td></tr>
<tr><td>2</td><td>セキュリティの維持</td><td>保守対象アプリケーションソフトウェアが搭載されているシステムのオペレーティングシステム（OS)、ミドルウェア等のパッチ等のリリースから1か月以内に開発環境での事前評価、運用環境への適用が完了しているか。</td></tr>
</table>

②受注者は、主管課と締結したサービスレベル合意書に基づき、サービスレベル管理指標毎の実施状況を毎月計測し、３か月毎に開催するサービスレベル報告会において、達成状況の報告を行うこと。
③受注者からのサービスレベル達成状況報告を基に、受注者と主管課は協議を行い、当該期間におけるサービスレベル合意書の達成度合いを判定する。委託金額の支払はサービスレベル合意書の達成度に合わせて決定する。未達成 SLA 項目が 90%未満の場合には受注者の負担で改善提案を行い、主管課の承認を得たうえで、対策を実施すること。
<table>
<tr><th>達成度合い</th><th>支払の割合</th><th>条件</th></tr>
<tr><td>A</td><td>100%(満額)</td><td>全 SLA 項目で指定条件達成</td></tr>
<tr><td>B</td><td>97%</td><td>指定条件を達成できない SLA 項目が SLA 項目数全体のうち 5%未満</td></tr>
<tr><td>C</td><td>94%</td><td>指定条件を達成できない SLA 項目が SLA 項目数全体のうち 5%以上 10%未満</td></tr>
<tr><td>D</td><td>90%</td><td>指定条件を達成できない SLA 項目が SLA 項目数全体のうち 10%以上</td></tr>
</table>
</td></tr>
<tr><td>案件・情報システムの特性等による留意点</td><td>複数年度にまたがるアプリケーション保守案件の場合、四半期ごとなど、頻繁にサービスレベル達成度の評価を実施するとともに、達成度合いが不十分な場合には体制の見直しを実施するなど、継続的な品質向上の取り組みが目指されている。</td></tr>
<tr><td>セキュリティに関する留意点</td><td>―</td></tr>
</table>

4. 障害対応

項目	内容
役務内容の概要	主管課又は運用事業者からのエスカレーションに対応して、現地対応（オンサイトサポート）を行う。
想定されるインプット（発注者側で用意）	・保守設計書 ・保守手順書 ・ハードウェア／ソフトウェアの取扱説明書、添付ドキュメント
成果物（受注者側で用意）	・障害報告書
仕様書に記載すべきポイント	原因究明時間や障害対応までの時間、原因判明率などのサービスレベル管理指標として記載する場合もある。 【1.基本的に記載すべき要求要件】 ・障害対応の実施 ・障害対応対応時間
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①運用事業者の一次切り分けを踏まえて、受注者は保守対象アプリケーションソフトウェアに関する障害原因の解析を行い、問題解決策又は問題回避策の検討を行い、主管課と協議の上、対策を実施する。 ②運用事業者の一次切り分けで障害原因の特定をできない場合、受注者は主管課からの指示によりハードウェア保守事業者、ソフトウェア保守事業者、運用事業者と連携して障害原因の特定、仮復旧等の支援を行う。 ③障害対応に係る対応時間は、平日 9:00～18:00（休日、祝日は除く）とする。ただし、受注者は時間外の対応について、主管課から協議があった場合は検討を行うものとする。
案件・情報システムの特性等による留意点	—
セキュリティに関する留意点	—

5. プログラム修正

項目	内容
役務内容の概要	プログラムの部分改修・機能追加・バグフィックスのための開発、テスト、本番環境へのリリース、パッチ適用、パッチ適用時のシステム影響分析
想定されるインプット （発注者側で用意）	手順書（保守手順書、運用手順書） 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面・帳票設計書、運用設計書、移行設計書、ハードウェア設計書 等） ソースコード　等 プロジェクト標準 テスト標準 コーディング規約 保守対象アプリケーションの変更要件
成果物 （受注者側で用意）	［修正版］手順書（保守手順書、運用手順書） ［修正版］設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面・帳票設計書、運用設計書、移行設計書、ハードウェア設計書 等） ［修正版］ソースコード　等 プログラムファイル テスト仕様書（単体テスト、結合テスト、総合テスト、受入テストの各仕様書） テスト結果報告書 リリース計画書 リリース手順書 リリース作業結果報告書
仕様書に記載すべきポイント	【1.基本的に記載すべき要求要件】 ・運用開始後に発見されたアプリケーションソフトウェアの問題に対するアプリケーションソフトウェアの修正 ・運用開始後に発生したアプリケーションソフトウェアのシステム基盤に対するパッチ適用可否の評価 ・制度変更等に伴う軽微なアプリケーションソフトウェアの部分改修および機能追加（設計書の修正、プログラム修正、テスト、移行等の付帯作業を含む） 【2.案件の種類・特性によって追記すべき要求要件】 ・アプリケーションソフトウェアに起因した性能問題に対処するためのアプリケーションソフトウェアの修正

項目	内容
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①受注者は主管課又は運用管理受託業者から発行されたインシデント管理票に基づき、保守対象アプリケーションソフトウェアの不具合の修正を本システムの設計・開発プロセスに基づき実施すること。ただし、設計・開発業者の瑕疵担保期間中はこの限りでない。 ②受注者は本システムの設計・開発プロセスに基づき、仕様書別紙に示された軽微な機能追加・修正を実施すること。 ③保守対象アプリケーションソフトウェアが稼働するシステムに使用されているオペレーションシステム（ＯＳ）、ミドルウェア等のパッチファイルがリリースされた場合、受注者は当該パッチファイルリリース後、1 か月以内に事前適用評価を実施すること。なお、事前適用評価は主管課が管理する保守環境において実施し、事前評価結果及びパッチ適用手順は文書化して速やかに主管課に報告すること。 【2.案件の種類・特性によって追記すべき要求要件】 ④評価済のオペレーションシステム（ＯＳ）、ミドルウェア等のパッチファイルは、主管課と協議の上、本システムの設計・開発プロセスに基づき速やかに運用環境への適用作業を実施すること。
案件・情報システムの特性等による留意点	アプリケーションの不具合は、さまざまな理由（原因判明が困難である、修正必要箇所が多岐に渡る、他システムへの影響がある等）から、修正が必要なことが判明してから実際の修正実施までの期間が長くかかることも想定される。そのため、修正実施までを役務要件として含めず、「アプリケーション不具合の判明時には担当者と協議の上アプリケーション修正の計画を立案する」という要件にとどめることも仕様書記載の上での選択肢となりえる。 「評価済ソフトウェアのパッチ適用」は、適用対象によって実施者が異なる。たとえば、PC や業務システムを搭載していないサーバ（たとえば、部門ファイルサーバ）に対する評価済パッチの適用は運用管理事業者が行うべき役務である。一方、業務システムを搭載しているサーバに対してはアプリケーション保守事業者が行うべき役務である。
セキュリティに関する留意点	－

6．技術支援

項目	内容
役務内容の概要	・主管課および運用事業者からの依頼に基づき、技術支援を実施する。
想定されるインプット （発注者側で用意）	・保守対象システムの設計書、保守手順書
成果物 （受注者側で用意）	・支援作業実施報告書
仕様書に記載すべきポイント	【１．基本的に記載すべき要求要件】 ・問い合わせへの対応 ・問題の切り分け支援 ・必要に応じた技術者の派遣（オンサイトサポート） 【2.案件の種類・特性によって追記すべき要求要件】 ・OS・ミドルウェア等のパッチ適用事前評価・影響分析 ・評価済パッチの適用等
仕様書記載上の例/説明	仕様書に記載する場合の例 ①受注者は、保守対象のアプリケーションソフトウェアが稼働しているシステムにおいて、運用開始後に追加・変更が必要となったシステム環境の見直し、パラメータ等の追加・変更、データベース定義等の見直し・変更、外字・システムコード等の追加・変更などの作業を実施すること。
案件・情報システムの特性等による留意点	パッチの情報提供と適用 情報システムに関する技術的問題、セキュリティ脆弱性（セキュリティホール）、ソフトウェアのバグ、パッチ及びバージョンアップ等に関する情報を、速やかに府省に報告すること。 また、府省の要求に応じて、パッチの適用可能性検証作業、適用作業パッチ等の適用作業及びソフトウェアの技術相談への対応を行うこと
セキュリティに関する留意点	－

6.6.3.3.納入成果物と提出のタイミング

アプリケーション保守業務に対する納入成果物と納入期限は以下の通りである。各成果物の正式名称、納入期限に関しては実態に即して記載をする必要がある。

役務作業	納入成果物	納入期限
1. 設計･開発事業者からの引継ぎ	引継実施報告書	引継完了後 1 週間以内
2. 保守計画策定	実施計画書	契約締結後 2 週間以内
3. サービスレベル管理	サービスレベル合意書 サービスレベル管理計画書	契約締結後 14 営業日以内
	サービスレベル管理結果報告書	サービスレベル計測期間毎、指定する期日
4. 障害対応	障害報告書	障害対応完了後 1 週間以内
5. プログラム修正	作業実施計画書	作業着手 14 日以上前
	［修正版］手順書（保守手順書、運用手順書）、［修正版］設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書 等）、［修正版］ソースコード等、プログラムファイル、テスト仕様書（単体テスト、結合テスト、総合テスト、受入テストの各仕様書）、テスト結果報告書、リリース計画書、リリース手順書、リリース作業結果報告書	随時（リリース完了後 14 日以内、又は検収時）
6. 技術支援	支援作業実施報告書	作業完了後 1 週間以内

6.6.3.4.想定されるインプット

受注者(もしくは提案者)に対して事前に提示すべきインプット、タイミングは下記の通りである。各インプットの正式名称、納入期限は実態に即して記載をする必要がある。

役務作業	インプット	インプットを提示するタイミング
1. 設計･開発事業者からの引継ぎ	保守計画書（案)、保守設計書、保守手順書、保守ツール、引継実施計画書（案）	設計･開発事業者からの引継実施時
2. 保守計画策定	保守計画（案） サービスレベル合意書（案） サービスレベル管理指標（案） 役割分担表（SOW）	調達仕様書に記載、又は別添資料として添付する
	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書、システム環境定義書等）	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
3. サービスレベル管理	サービスレベル合意書（案） サービスレベル管理指標（案）	調達仕様書に記載、又は別添資料として添付する
4. 障害対応	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書、システム環境定義書等） ソースコード	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
5. プログラム修正	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書、システム環境定義書等） ソースコード	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
6. 技術支援	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書、システム環境定義書等） ソースコード 保守作業量の目安となる情報	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。

6.6.3.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。
調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表で提示することが必要である。

○：主担当、△：支援、助言

作業項目	主管課	HW 保守事業者	SW 保守事業者	AP 保守事業者	運用事業者	iDC 事業者	ヘルプデスク事業者
ハードウェア、パッケージソフトウェア、ネットワーク等の運用保守計画の企画、調達	○	△		△	△	△	－
ハードウェアのオンサイトサポート	－	○	-	－	△	△	－
パッケージソフトウェアのパッチ提供、オフサイトサポートの実施	－	－	○	－	△	△	－
ネットワークのオンサイトサポート	－	－	－	－	○	△	－
システムの日常オペレーション	－	－	－	－	○	△	－
システム、ネットワーク監視	－	－	－	－	○	△	－
セキュリティ監視	－	－	－	－	○	△	－
利用者からの問い合わせ対応	○	－	－	－	－	－	○
主管課からの問い合わせ、統合ヘルプデスクからエスカレーション対応	－	○	○	○	○	○	○
問題発生時の一次切り分け	△	△	△	△	○	△	－
問題発生時の二次対応（ハードウェア障害）	△	○	△	△	△	△	－
問題発生時の二次対応（ソフトウェア／アプリケーションソフトウェア障害）	△	△	△	○	△	△	－
問題発生時の二次対応（iDC 設備障害）	△	△	△	△	△	○	－
障害発生時のシステムリカバリ処理	△	△	－	○	○	－	－
アプリケーションソフトウェアの保守	△	－	－	○	－	－	－
運用管理情報の収集、分析、報告、提言	△	△	－	△	○	△	－
消耗品の管理	－	－	－	－	○	－	－

表 6.6.3.5.1 運用・保守事業者の役割分担（例）

6.6.4.システム基盤保守

6.6.4.1.調達分野の定義

システム基盤保守は、「EIP」「公開Webサーバ」「グループウェア、ファイルサーバ、メールサーバ」「統合アカウント管理・認証・認可(アクセス制御)」「統合ディレクトリ」「WAN・省内LAN、DNS/DHCP/Proxy、リモートアクセス」「ネットワーク回線」など、技術参照モデルの「第5章技術ドメイン解説」に含まれる技術に対する保守役務である。

なお、これらの保守は機器の設置、セットアップなどの機器の導入と環境の整備も同じ契約の中で調達する場合があるが、本項の記載では保守に関わる役務部分についてのみ記載している。

図 6.6.4-1 役務調達の分類における対応箇所

6.6.4.2.仕様書に記載すべき役務内容

6.6.4.2.1.代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応するSLCP-2007のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCPのアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

【システム基盤保守】

役務作業	役務の概要	SLCPのアクティビティ	調達基本指針に対応する仕様書の章・節
1. 設計・開発事業者からの引継ぎ	設計・開発事業者からの引継ぎ	1.8.1.1 開発プロセスからの引き継ぎ	11章　保守要件定義（ただし、(1)(2)いずれにも該当しない）
2.保守計画策定	システム基盤保守計画書（保守作業計画、平常時・緊急時の連絡先を記した体制表等を含む）の策定	1.8.1 プロセス開始の準備（保守プロセス）	
3.サービスレベル管理	SLA締結、SLA指標に関する記録、SLA未達成時の改善の実施	―	
4.障害対応	運用事業者が解決できないシステム障害等に対して、ハードウェア保守事業者、ソフトウェア保守事業者、運用事業者と連携して実施する障害対応	1.8.2 問題把握及び修正分析 1.8.3 修正の実施 1.8.4 保守レビュー及び受入れ	
5.システム基盤ソフトウェアのアップデート	サービスを継続的に提供するために必要となるソフトウェア保守等の作業	1.8.2 問題把握及び修正分析 1.8.3　修正の実施 1.8.4 保守レビュー及び受入れ	
6.技術支援	システムの運用に必要となるシステムエンジニアの各種作業	1.8.3 修正の実施 1.8.4 保守レビュー及び受入れ	

6.6.4.2.2.各役務内容に関する説明及び仕様書上の記載例

1.　設計･開発事業者からの引継ぎ

項目	内容
役務内容の概要	設計・開発事業者からの引継ぎ
想定されるインプット （発注者側で用意）	【設計・開発事業者が作成した運用・保守関係の成果物】 ・　保守計画書（案） ・　保守設計書 ・　保守手順書 ・　保守ツール ・　引継実施計画書
成果物 （受注者側で用意）	・　引継実施報告書 ・　保守計画書 ・　保守体制表
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・　引継実施報告書の作成 ・　新システムの各本番稼動前に、設計・開発事業者からの引継ぎを実施 ・　保守設計書・保守手順作成資料に関して疑義が生じた場合、設計・開発事業者に対し、問い合わせや修正依頼を実施 ・　保守手順作成資料に基づき、保守手順書を作成
仕様書記載上の例/説明	○保守業者への引継ぎ ▪　受託者は契約完了後速やかに担当職員と協議し、平成○年○月末までに受託者の負担と責任において、保守対象のシステム基盤の内容及び保守業務等に関する引継ぎを設計開発事業者から受けること。 ▪　受託者は保守に関する引継ぎを踏まえて、保守体制を整備し、保守計画書を作成すること。
案件・情報システムの特性等による留意点	―
セキュリティに関する留意点	―

2. システム基盤保守計画の策定

項目	内容
役務内容の概要	システム基盤保守計画書（保守作業計画、平常時・緊急時の連絡体制を記した体制表　等を含む）を主管課に提出し、承認を得る
想定されるインプット （発注者側で用意）	【1.基本的に提示すべきインプット】 ・保守要領 ・保守手順書 ・役割分担表（当該システムの関連事業者、発注者） 【2.案件の種類・特性によって追加提示が必要となるインプット】 ・サービスレベル管理指標（案）
成果物 （受注者側で用意）	・システム基盤保守計画書
仕様書に記載すべきポイント	保守計画策定に関する要求事項を記載する。 【1.基本的に記載すべき要求要件】 事前に「保守計画書」を作成及び納入し、発注者の承認を得る。 ・業務実施の手順を詳細に定義 ・体制、役割分担、連絡方法などの計画を策定
仕様書記載上の例/説明	仕様書に記載する場合の例 ①受注者は、「本調達仕様書」及び別途提示する「保守設計書」、「保守手順書」等に基づき、定期保守、システムメンテナンス作業などの保守計画を作成・納入し、主管課の承認を得ること。 ②保守作業計画はシステム（サービス）停止の回避等、業務に支障をきたさないよう十分に配慮した作業計画であること。業務への影響がある保守作業は実施日を調整の上、休日等の対応にも応じること。 ③受注者は、保守対象機器の障害発生時及び主管課の求めに対して、標準保守対応時間に迅速な保守対応ができる体制を構築し、主管課の承認を得ること。なお、保守要員は、保守対象システム基盤を含む保守対象システム全体に関する十分な知識、経験等を有する技術者であること。
案件・情報システムの特性等による留意点	運用事業者、関連システムの関係者など、関係する事業者との役割分担、各事業者の責任範囲を明確に示す必要がある。
セキュリティに関する留意点	―

3. サービスレベル管理

項目	内容
役務内容の概要	SLA の締結、サービスレベルの報告、改善のための取り組み等を実施 なお、サービスレベル管理は全ての案件に適用する必要はないので、調達時に SLA の適用が必要か否か、十分に検討を行うこと。
想定されるインプット （発注者側で用意）	・サービスレベル管理指標（案） ・サービスレベル合意書（SLA）（案）
成果物 （受注者側で用意）	・サービスレベル合意書（SLA） ・保守報告書 ・サービスレベル報告書
仕様書に記載すべきポイント	【1.基本的に記載すべき要求要件】 なし 【2.案件の種類・特性によって追記すべき要求要件】 保守業務実施の上で、受注者と発注者の間で締結する SLA についての要件を記載するとともに、サービスレベル管理指標に関して、両者で協議をする余地がある旨を記載する。 また、SLA 遵守を特に厳しく求める場合は、定期的なレビューの実施や、遵守できなかった場合の業務要件について記載する。 ・府省と保守事業者でのサービスレベル管理指標に関する協議の実施 ・バージョンアップ頻度、障害対応時間などの SLA 項目の定義や注釈 ・定期的な SLA の遵守結果のレビュー実施 ・SLA が遵守できなかった場合の対応要件（無償対応や改善のための取り組み）

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>仕様書記載上の例/説明</td><td>仕様書に記載する場合の例

【2.案件の種類・特性によって追記すべき要求要件】
①本調達では受注者の提供する保守の高い品質が維持されていることを検証するため、受注者と協議のうえ、サービスレベル合意書（Service Level Agreement）を締結する。受注者は、本仕様書が示すサービスレベル管理指標を基にサービスレベルの維持・向上に資するサービスレベル合意書案を策定し、提案書にて提示すること。

<table>
<tr><th>No</th><th>サービスレベル管理指標</th><th>説明</th></tr>
<tr><td>1</td><td>アプリケーションソフトウェアの修正</td><td>アプリケーションの欠陥が発見されてから1か月以内に対処が完了しているか。</td></tr>
<tr><td>2</td><td>セキュリティの維持</td><td>保守対象アプリケーションソフトウェアが搭載されているシステムのオペレーティングシステム（OS）、ミドルウェア等のパッチ等のリリースから1か月以内に開発環境での事前評価、運用環境への適用が完了しているか。</td></tr>
</table>

②受注者は、主管課と締結したサービスレベル合意書に基づき、サービスレベル管理指標毎の実施状況を毎月計測し、3か月毎に開催するサービスレベル報告会において、達成状況の報告を行うこと。
③受注者からのサービスレベル達成状況報告を基に、受注者と主管課は協議を行い、当該期間におけるサービスレベル合意書の達成度合いを判定する。委託金額の支払はサービスレベル合意書の達成度に合わせて決定する。未達成SLA項目が90%未満の場合には受注者の負担で改善提案を行い、主管課の承認を得たうえで、対策を実施すること。</td></tr>
</table>

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td></td><td><table>
<tr><th>達成度合い</th><th>支払の割合</th><th>条件</th></tr>
<tr><td>A</td><td>100%(満額)</td><td>全SLA項目で指定条件達成</td></tr>
<tr><td>B</td><td>97%</td><td>指定条件を達成できないSLA項目が3ヶ月の合計SLA項目数全体のうち5%未満</td></tr>
<tr><td>C</td><td>94%</td><td>指定条件を達成できないSLA項目が3ヶ月の合計SLA項目数全体のうち5%以上10%未満</td></tr>
<tr><td>D</td><td>90%</td><td>指定条件を達成できないSLA項目が3ヶ月の合計SLA項目数全体のうち10%以上</td></tr>
</table></td></tr>
<tr><td>案件・情報システムの特性等による留意点</td><td>―</td></tr>
<tr><td>セキュリティに関する留意点</td><td>―</td></tr>
</table>

4. 障害対応

項目	内容
役務内容の概要	主管課又は運用事業者からのエスカレーションに対応して、現地対応（オンサイトサポート）を行う。
想定されるインプット （発注者側で用意）	・保守設計書 ・保守手順書 ・ハードウェア／ソフトウェアの取扱説明書、添付ドキュメント
成果物 （受注者側で用意）	・障害報告書
仕様書に記載すべきポイント	原因究明時間や障害対応までの時間、原因判明率などのサービスレベル管理指標として記載する場合もある。 【1.基本的に記載すべき要求要件】 ・障害対応の実施 ・障害対応対応時間
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①運用事業者の一次切り分けを踏まえて、受注者は保守対象アプリケーションソフトウェアに関する障害原因の解析を行い、問題解決策又は問題回避策の検討を行い、主管課と協議の上、対策を実施する。 ②運用事業者の一次切り分けで障害原因の特定をできない場合、受注者は主管課からの指示によりハードウェア保守事業者、ソフトウェア保守事業者、運用事業者と連携して障害原因の特定、仮復旧等の支援を行う。 ③障害対応に係る対応時間は、平日 9:00～18:00（休日、祝日は除く）とする。ただし、受注者は時間外の対応について、主管課から協議があった場合は検討を行うものとする。
案件・情報システムの特性等による留意点	システムの冗長化が図られ、障害発生時にも継続運用が可能な場合は、担当職員と協議の上で可及的速やかな対応を実施しないといった保守仕様も想定される。
セキュリティに関する留意点	―

5．システム基盤ソフトウェアのアップデート

項目	内容
役務内容の概要	システム基盤ソフトウェアの不具合、脆弱性対策、機能強化等のため、システム基盤ソフトウェアのアップデート、パッチ適用等の作業を実施する。
想定されるインプット （発注者側で用意）	手順書（保守手順書、運用手順書） 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面・帳票設計書、運用設計書、移行設計書、ハードウェア設計書 等）、 ソースコード 等
成果物 （受注者側で用意）	［修正版］手順書（保守手順書、運用手順書） ［修正版］設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面・帳票設計書、運用設計書、移行設計書、ハードウェア設計書 等）、 ［修正版］ソースコード 等、 プログラムファイル、 テスト仕様書、 テスト結果報告書、 リリース計画書、 リリース手順書、 リリース作業結果報告書　など
仕様書に記載すべきポイント	【1.基本的に記載すべき要求要件】 ・保守環境での事前評価の実施 ・関連システム／ソフトウェアの動作検証 ・設計書、手順書等の改版 ・構成管理の実施
仕様書記載上の例/説明	仕様書に記載する場合の例 【1.基本的に記載すべき要求要件】 ①受注者は保守対象のシステム基盤及びシステム基盤ソフトウェアの不具合情報、脆弱性情報、主管課から示されたインシデント管理票等に基づき、システム基盤ソフトウェアのアップデートを実施すること。アップデートの実施にあたっては、予め保守環境で事前評価を実施の上、主管課の承認を得たのちにアップデートを実施すること。 ②システム基盤ソフトウェアのアップデート検証時には、システム基盤上又はシステム基盤と連携して動作するシステム／ソフトウェアの動作検証も同時に実施すること。 ③アップデートの実施にあたっては本プロジェクトの構成管理プロ

項目	内容
	セスに従って、設計書・手順書等の改版を実施すること。また、成果物は構成管理プロセスに従って、管理すること。
案件・情報システムの特性等による留意点	
セキュリティに関する留意点	セキュリティパッチの情報提供と適用 情報システムに関する技術的問題、セキュリティ脆弱性（セキュリティホール）、ソフトウェアのバグ、パッチ及びバージョンアップ等に関する情報を、速やかに府省に報告させる。 また、府省の要求に応じて、パッチの適用可能性検証作業、適用作業パッチ等の適用作業及びソフトウェアの技術相談への対応を行うこと。

6. 技術支援

項目	内容
役務内容の概要	・パッチ適用に伴う事前評価作業、運用環境へのパッチ適用作業、、ソースコード変更を伴わない軽微な設定変更、外部システムやネットワークの更改等に伴う影響分析等
想定されるインプット （発注者側で用意）	・保守対象システムの設計書、保守手順書
成果物 （受注者側で用意）	［修正版］ソースコード　等、プログラムファイル、テスト仕様書、テスト結果報告書、リリース計画書、リリース手順書、リリース作業結果報告書
仕様書に記載すべきポイント	【１．基本的に記載すべき要求要件】 ・ソースコード変更を伴わない軽微な設定変更 ・外部システムやネットワークの更改等に伴う影響分析 等 ①「EIP」 ・データベースのテーブルの削除・新規作成、データのインポートなどのデータベースのメンテナンス ・外字フォントの保守 ②「公開 Web サーバ」 ・サーバ証明書失効時の証明書入れ替え ・脆弱性情報等に基づく、サーバセキュリティ設定の見直し ③「グループウェア、ファイルサーバ、メールサーバ」 ・ユーザアカウント情報の登録・更新・削除・ ④「統合アカウント管理・認証・認可(アクセス制御)」 ・ユーザアカウント情報の登録・更新・削除 ⑤「統合ディレクトリ」 ・ユーザアカウント情報の登録・更新・削除 ⑥「WAN・省内 LAN、DNS/DHCP/Proxy、リモートアクセス」 ・DNS サーバへの登録・更新・削除
仕様書記載上の例/説明	仕様書に記載する場合の例 【１．基本的に記載すべき要求要件】 受注者は、保守対象のシステム基盤ソフトウェアが稼働している OS、ミドルウェア等のセキュリティパッチやアップデートが公開された場合、適用の要否を検討こと。また、適用が必要と判断された場合はパッチ等の適用により、不具合が発生しないことを保守環境等で事前評価を行い、主管課に報告のうえ、運用環境に適用すること。

項目	内容
	【2.案件の種類・特性によって追記すべき要求要件】 ［ＥＩＰ関連］ 受注者は主管課の依頼があったアプリケーションをポートレットに組み込めるよう、登録を行うこと。 受注者は EIP に登録するデータ等のメンテナンスを実施すること。 ［公開Ｗｅｂサーバ関連］ ・ 脆弱性情報等を随時確認し、公開 Web サーバのセキュリティレベルが低下しないよう、セキュリティ設定を定期的に見直すこと。 ［グループウェア、ファイルサーバ、メールサーバ関連］ ・ 職員の採用、退職、異動等に伴うグループウェア、ファイルサーバ、メールサーバの権限設定を適切に行うこと。 ［統合アカウント管理・認証・認可(アクセス制御)関連］ ・ 職員の採用、退職、異動等に伴うユーザアカウントの追加・変更・削除を適切に実施すること。 ［統合ディレクトリ関連］ ・ 省内システムの追加、変更、廃止等に伴う統合ディレクトリの設定を確実に実施すること。 ［WAN・省内 LAN、DNS/DHCP/Proxy、リモートアクセス関連］ ・ 省内システムの追加、変更、廃止等に伴う WAN・省内 LAN、DNS/DHCP/Proxy 等の設定の変更を実施すること。
案件・情報システムの特性等による留意点	
セキュリティに関する留意点	—

6.6.4.3.納入成果物と提出のタイミング

システム基盤保守業務に対する納入成果物、タイミングは下記の通りである。各成果物の正式名称、納入期限は実態に即して記載をする必要がある。

役務作業	納入成果物	納入期限
1. 設計・開発事業者からの引継ぎ	引継実施報告書	引継完了後 1 週間以内
2. 保守計画策定	保守実施計画書	契約締結後 2 週間以内
3. サービスレベル管理	サービスレベル合意書 サービスレベル管理計画書	契約締結後 14 営業日以内
	サービスレベル管理結果報告書	サービスレベル計測期間毎、指定する期日
4. 障害対応	保守報告書 サービスレベル報告書（※障害対応が SLA の対象になった場合）	保守報告書：月次 サービスレベル報告書：検収時 or　四半期ごと
5. システム基盤ソフトウェアのアップデート	作業実施計画書	作業実施 14 営業日以上前
	［修正版］手順書（保守手順書、運用手順書）、［修正版］設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面・帳票設計書、運用設計書、移行設計書、ハードウェア設計書　等）、［修正版］ソースコード　等、プログラムファイル、テスト仕様書、テスト結果報告書、リリース計画書、リリース手順書、リリース作業結果報告書	随時（リリース完了後 14 日以内、又は検収時）
6. 技術支援	作業実施計画書	作業実施 14 営業日以上前
	［修正版］ソースコード　等、プログラムファイル、テスト仕様書（単体テスト、結合テスト、総合テスト、受入テストの各仕様書）、テスト結果報告書、リリース計画書、リリース手順書、リリース作業結果報告書	作業実施後 7 営業日以内

6.6.4.4.想定されるインプット

受注者(もしくは提案者)に対して事前に提示すべきインプット、タイミングを記載すると下記の通りである。各インプットの正式名称、納入期限は実態に即して記載をする必要がある。

役務作業	インプット	インプットを提示するタイミング
1. 設計･開発事業者からの引継ぎ	保守計画書（案)、保守設計書、保守手順書、保守ツール、引継実施計画書（案）	設計･開発事業者からの引継実施時
2. 保守計画策定	保守計画（案） サービスレベル合意書（案） サービスレベル管理指標（案） 役割分担（SOW）	調達仕様書に記載、又は別添資料として添付する
	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、 ・ハードウェア設計書 等）	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
3. サービスレベル管理	サービスレベル合意書（案） サービスレベル管理指標（案）	調達仕様書に記載、又は別添資料として添付する
4. 障害対応	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書、システム環境定義書等） ソースコード	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
5. システム基盤ソフトウェアのアップデート	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書、システム環境定義書等） ソースコード	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。
6. 技術支援	保守手順書 運用手順書 設計書（保守設計書、運用設計書、システム設計書、プログラム設計書、データベース設計書、画面･帳票設計書、運用設計書、移行設計書、ハードウェア設計書 等） 保守作業量の目安となる情報 ソースコード　等	応札期間中：応札者に閲覧を許可する。 契約締結後：受注者に貸与する。

6.6.4.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表で提示することが必要である。

○：主担当、△：支援、助言

作業項目	主管課	HW 保守事業者	SW 保守事業者	AP 保守事業者	運用事業者	iDC 事業者	ヘルプデスク事業者
ハードウェア、パッケージソフトウェア、ネットワーク等の運用保守計画の企画、調達	○	△		△	△	△	−
ハードウェアのオンサイトサポート	−	○	-	−	△	△	−
パッケージソフトウェアのパッチ提供、オフサイトサポートの実施	−	−	○	−	△	△	−
ネットワークのオンサイトサポート	−	−	−	−	○	△	−
システムの日常オペレーション	−	−	−	−	○	△	−
システム、ネットワーク監視	−	−	−	−	○	△	−
セキュリティ監視	−	−	−	−	○	△	−
利用者からの問い合わせ対応	○	−	−	−	−	−	○
主管課からの問い合わせ、統合ヘルプデスクからエスカレーション対応	−	○	○	○	○	○	○
問題発生時の一次切り分け	△	△	△	△	○	△	−
問題発生時の二次対応（ハードウェア障害）	△	○	△	△	△	△	−
問題発生時の二次対応（ソフトウェア／アプリケーションソフトウェア障害）	△	△	△	○	△	△	−
問題発生時の二次対応（iDC 設備障害）	△	△	△	△	△	○	−
障害発生時のシステムリカバリ処理	△	△	−	○	○	−	−
アプリケーションソフトウェアの保守	△	−	−	○	−	−	−
運用管理情報の収集、分析、報告、提言	△	△	−	△	○	△	−
消耗品の管理	−	−	−	−	○	−	−

表 6.6.4.5.1 運用・保守事業者の役割分担（例）機器調達付帯作業

6.7.機器調達付帯作業

6.7.1.調達分野の定義

機器調達付帯作業とは、情報システムを実現するために必要な機器（ハードウェアと不可分な OS 等の既製のソフトウェアを含む）に付帯する役務を指す（図表.6.7.1 参照）。

尚、機器調達の場合は機器の設置、セットアップなどの機器の導入と環境の整備に加えその後の保守も同じ契約の中で調達する場合があるが、本項の記載では機器の導入･設置に関わる役務部分についてのみ記載している。

図 6.7-1 役務調達の分類における対応箇所

6.7.2.仕様書に記載すべき役務内容

6.7.2.1.代表的な役務作業の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [11]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ･モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[12]の項目との対応も記載している。実際の仕様書の作成

[11] 独立行政法人　情報処理推進機構　共通フレーム 2007
ソフトウェアライフサイクルプロセス　SLCP-JCF 2007

[12] 総務省　情報システムに関わる政府調達の基本指針　2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

にあたっては、府省庁の全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務作業の概要	SLCP の アクティビティ	調達基本指針に対応する仕様書の章･節 （及びそのタイトル）
1.計画策定	作業内容･スケジュール･工程･実施体制（役割分担）の策定、実施計画書の作成 進捗状況の管理、担当者へのレビュー	1.2.4：計画立案 1.2.5：実行及び管理 1.2.6： レビュー及び評価	12 章　作業の体制及び方法 （1）作業体制 （3）導入
2.関係者への事前説明･調整	関連事業者･府省庁に対する事前説明･事前調整	3.2.2： 環境構築プロセス	12 章　作業の体制及び方法 （3）導入
3.現地調査･設計	機器導入拠点の現地調査 現地調査報告書･施行図面の作成 「現地作業計画書」の作成 機器設置レイアウト図･ラックレイアウト図･ネットワーク敷設図（ネットワークを含む場合）等の図面、セキュリティ設計書･ネットワーク設計書等の各種設計書の作成･提出	3.2.2 環境構築プロセス 3.2.1 プロセス開始の準備 (環境整備プロセス)	12 章　作業の体制及び方法 （3）導入
4.機器導入･設置作業	電源･空調等の工事 機器の搬入･設置	3.2.2 環境構築プロセス	12 章　作業の体制及び方法 （3）導入
5.機器のセットアップ	設計書に基づくネットワーク敷設（ネットワークを含む場合）、ソフトウェアのインストール･設定、他システムとの接続作業	1.6.12 ソフトウェア導入プロセス	12 章　作業の体制及び方法 （3）導入
6.動作確認･テスト	設置したハードウェア、ソフトウェア、ネットワーク（ネットワークを含む場合）の動作確認テストの実施 システム開発事業者において実施するテストの支援	2.4.1 プロセス開始の準備 2.4.2　検証、 2.5.1 プロセス開始の準備、 2.5.2　妥当性の確認	8 章　テスト要件定義
7.移行業務	現行体制からのデータ･システム、･業務等の移行作業又は作業	1.8.5　移行プロセス	9 章　移行要件定義 (1)移行に関わる要件

役務作業	役務作業の概要	SLCPの アクティビティ	調達基本指針に対応する仕様書の章・節 （及びそのタイトル）
	支援		
8.運用・保守事業者等への情報提供	運用・保守等事業者に対する機器・ソフトウェアの設定情報、操作方法等の情報提供	1.6.13 ソフトウェア受入支援	9章　移行要件定義 (2)教育に関わる要件
9.利用者への情報提供・教育	一般職員及びシステム担当者に対する、システムの操作方法の教育 （対象システムを一般職員が活用する場合）	1.6.13 ソフトウェア受入支援	9章　移行要件定義 (2)教育に関わる要件
10.検収	必要な納入物一式の準備・納入 府省庁の求める受入試験への対応	1.2.7 納入及び完了	12章　作業の体制及び方法 （3）導入

6.7.2.2.各役務内容に関する説明及び仕様書上の記載例

1. 計画策定

項目	内容
役務内容の概要	作業内容、スケジュール、作業場所、役割分担を含めた実施体制を検討し、計画書を作成する。
想定されるインプット（発注者側で用意）	・ スケジュール全体像 ・ 役割分担表
成果物（受注者側で用意）	・ 実施計画書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 計画書に含めるべき作業内容 ・ 作業担当者における役割分担 ・ 作業体制 ・ 作業時間帯、作業場所等に関する指定及び制約条件等 **【2.案件の種類・特性によって追記すべき要求要件】** ・ 作業者に求める資格 ・ 経験など受注側の体制に求める要件 ・ 作業時間・作業場所に関する詳細ルール ・ 拠点によって作業日時等の条件面が異なる場合には、各拠点における作業計画の提出
仕様書記載上の例/説明	○実施計画書作成 受注者は、機器の導入に先立ち、作業内容、作業体制及びスケジュール等を記載した「実施計画書」を作成すること。 (1) 実施計画書作成について イ. 「実施計画書」は、「表○○ 導入作業の役割分担表」に示す作業全てを含むこと。 ロ. 「実施計画書」の作成において、外部関連事業者との連携が必要な作業の調整については、本省と協議すること。また、必要となる調整作業を支援すること。 (2) 作業時間について 搬入・設置作業は、平日の業務時間内を基本とすること。
案件・情報システムの特性等による留意点	・ 府省庁によっては導入計画書、体制表を分けて提出を求める場合も存在する。こうした点に関しては各府省庁で定められている調達方針・ガイドラインに沿うよう仕様書に記載する事が望ましい。 ・ 特定の経験やスキル等を必要とする案件については、特に求める担当者の要件について詳細に記載する必要がある。

	・ 導入作業等を行う拠点が多数に渡る場合については、それぞれの拠点での担当者一覧や連絡先等の提出や、現地作業の統一ルール等を定める必要がある。
セキュリティに関する留意点	―

2. 関係者への事前説明･調整

項目	内容
役務内容の概要	関連事業者・府省庁に対する事前説明、事前の調整事項に関する検討を実施する。
想定されるインプット （発注者側で用意）	・ 各拠点・関連事業者の連絡先 ・ 導入対象拠点の一覧 ・ 導入機器等一覧
成果物 （受注者側で用意）	・ 事前調整・説明会の資料および議事録（支援の場合はドラフト）
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 事前調整を実施すべきとする旨 ・ 事前調整すべき項目（具体的に記載すること） ・ 事前調整すべき関係者（対象人数の想定を記載すること） **【2.案件の種類・特性によって追記すべき要求要件】** ・ 説明会等の会議体の開催（又は参加）をすべき場合はその旨を記載する ・ 説明会等の会議体の対象となる参加者・説明内容
仕様書記載上の例/説明	○納入に当たっての事前作業条件 (ｱ) 納入に当たっては、現地での説明会等へ参加し、納入機器の詳細や、スケジュール、その他必要な説明を行うこと。 (ｲ) 再利用製品の設置場所や電源の確保等、設定変更に当たって現地担当者との事前調整が必要な事項を抽出すること。 (ｳ) 前項で抽出した事項について、事前に調整を行うこと。
案件・情報システムの特性等による留意点	端末等の多数拠点への導入の場合については、拠点ごとに関係者が存在するため、調整すべき関係者について仕様書上に記載する必要がある。 また、前年度の機器（再利用製品）などが残る場合には前年度の端末導入事業者や現地担当者等との調整が必要となるため、その旨も記載する必要がある。
セキュリティに関する留意点	－

3. 現地調査・設計

項目	内容
役務内容の概要	機器を導入する拠点に対する現地調査を実施し、現地調査報告書を作成の上、施工図面を作成する
想定されるインプット （発注者側で用意）	・ 各府省庁で定めるセキュリティポリシー ・ 政府機関の情報セキュリティ対策のための統一基準 ・ 現行のものに関する、施工図面、機器設置レイアウト図、ラック搭載図、配線図などの各種設計書
成果物 （受注者側で用意）	・ 現地調査計画書 ・ 現地調査報告書 ・ 施工図面、機器設置レイアウト図、ラック搭載図、配線図などの各種設計書
仕様書に記載すべきポイント	**【1.基本的に記載すべき要求要件】** ・ 仕様書の要求要件から適切な機器・ソフトウェアを選定 ・ 必要となる現地調査 ・ 現地調査を実施した結果、設計 ・ 作成すべき図面等のアウトプット ・ 現地調査の実施及びアウトプット提出のタイミング ・ 現地調査実施にあたっての制約事項 **【2.案件の種類・特性によって追記すべき要求要件】** ・ 統一基準府省庁のセキュリティポリシー等からセキュリティ要件定義 ・ 設計を実施すべき場合は、"セキュリティ要件定義・設計"を要求要件に含める
仕様書記載上の例/説明	**仕様書に記載する場合の例** ⑴ 設置場所については、各種調査等を行った上で、「機器設置レイアウト図」及び「ラック搭載図」を作成すること。 ⑵ 電源及びＬＡＮケーブル敷設作業実施に必要となる現地調査を行うこと。現地調査や各種調査は、当局から切替えを行うサイトに対して提示する「システム切替作業実施計画」にしたがって行うものとする。
案件・情報システムの特性等による留意点	他府省庁管轄システムとの接合などを実施する場合は、他府省庁の担当局と調整を行ったうえで、ネットワーク設計書を作成する旨を記載する必要がある。その場合は、関係する調整先を明記すること。
セキュリティに関する留意点	セキュリティ設計 「政府機関の情報セキュリティ対策のための統一基準」、及び各府省の情報セキュリティポリシーに準拠してセキュリティ設計書を作成し、それに準じた情報セキュリティ対策を実施すること。

4. 機器導入・設置作業

項目	内容
役務内容の概要	電源・空調等の工事、機器の搬入・設置を行う。
想定されるインプット (発注者側で用意)	・ 現行のものに関する、施行図面・機器設置レイアウト図・ラック搭載図・配線図・その他各種設計書 ・ 電源使用状況に関する資料
成果物 (受注者側で用意)	・ 工事結果に関する、施工図面・機器設置レイアウト図・ラック搭載図・配線図・その他各種設計書の変更書
仕様書に記載すべきポイント	搬入、設置作業における要件について記載する。搬入の際の条件、設置する際の条件、及び必要となる工事等について必要な要件を記載する。システム停止の可否やタイミングなどは前提条件として記載する必要がある。また、搬入搬出にあたっての責任分界点、養生の必要性については、別途作業の前提条件として記載する方法も想定される。 **【1.基本的に記載すべき要求要件】** ・ 機器導入において実施すべき作業 ・ 導入における前提条件 **【2.案件の種類・特性によって追記すべき要求要件】** ・ 機器設置における具体的な設置条件 ・ 施工条件 ・ LAN 等のネットワークの物理的な接続
仕様書記載上の例/説明	**仕様書に記載する場合の例** 1. 機器導入作業内容 受注者は、機器の導入において、以下に示す作業を実施すること。 (1) 搬入・設置 ア. 調達する機器の搬入・設置作業 イ. 機器の搬入・設置作業をするための申請 ウ. 機器の搬入・設置を行うための事前調査 エ. 搬入・設置作業に際し必要となる部材等の手配 オ. 設置完了後に不要となった、機器の梱包物、搬入の際に使用した養生品及びその他資材の撤去および廃棄 カ. 搬入時に発生した損害への対応 キ. 適切な耐震対策の施工
案件・情報システムの特性等による留意点	大規模な分離調達案件の場合、機器の設置・接続等の責任分界点が不明確になる恐れがあることから、予め役割分担表を作成するなどして明確化しておく必要がある。
セキュリティに関する留意点	―

5. 機器のセットアップ

項目	内容
役務内容の概要	作成した各種の設計書から、ネットワークの設定、ソフトウェアのインストール、設定、他システムとの接続等に必要な機器の設定等を実施し、機器を使用可能な状態にする。
想定されるインプット （発注者側で用意）	・ ハードウェア要件、ソフトウェア要件、ネットワーク要件、運用保守要件
成果物 （受注者側で用意）	・ 環境定義書
仕様書に記載すべきポイント	設置した機器を利用可能にするための各種設定、調整作業に関する要件を記載する。記載にあたっては、当該案件の受注者とその他の調達案件受注者との役割分担を十分認識の上、案件ごとに必要となる作業要件を記載する事。 **【1.基本的に記載すべき要求要件】** ・ ハードウェア設定 ・ ソフトウェアのインストール（各ソフトウェアについて、設計・インストール・設定の担当者を役割分担表等で明確にする必要がある） ・ 設定 **【2.案件の種類・特性によって追記すべき要求要件】** ・ ネットワークの設定 ・ ネットワークへの接続 ・ バックアップ等付随する必要な作業
仕様書記載上の例/説明	**仕様書に記載する場合の例** 1. 機器セットアップ (ア) 本調達において納入する機器のハードウェアの設定、ソフトウェアのインストール及び設定、ネットワークの設定を行うこと。 (イ) 本システム用機器等に搭載されるソフトウェア等及びネットワーク機器のファームウェア類について修正プログラムを適用すること。ただし、適用の可否を協議の上、決定すること。 (ウ) 改修業者と十分な調整を行い、ネットワークの設定、ディスク割り付け等の各種環境の設定、セキュリティの設定及び納品されるすべてのソフトウェア等のインストール等設定作業を行うこと。
案件・情報システム	大規模な分離調達案件の場合、責任分界点が不明確になる恐れがあ

の特性等による留意点	ることから、予め役割分担表（6.7.5 参照）を作成するなどして明確化しておく必要がある。
セキュリティに関する留意点	・ セキュリティの設定・調整 現行システムに係わる手順書、導入方法や作成したセキュリティ設計書を用いて本システムに必要な環境設定、各種調整作業を行うこと。 ・ ウイルス定義ファイルの更新 ウイルスソフト・ウイルス定義ファイルが常に最新の状態にあるよう更新を行うこと。

6. 動作確認・テスト

項目	内容
役務内容の概要	設置したハードウェア、ソフトウェア、ネットワークの動作確認テスト、及びシステム開発事業者において行うテストの支援を実施する。
想定されるインプット （発注者側で用意）	・ 動作確認項目一覧 ・ 他機能群との連携方針等のテスト実施に必要な情報
成果物 （受注者側で用意）	・ テスト仕様書 ・ テスト結果報告書（動作試験報告書）
仕様書に記載すべきポイント	設置した機器、ソフトウェアの動作検証として実施すべき検査とその要件、対象を記載する。発注者側から提示すべき書類、テスト結果を受け報告すべき書類等が存在する場合は併せて明記する事。 **【1.基本的に記載すべき要求要件】** ・ 動作確認・テスト対象 ・ 動作確認・テストの実施及び検証 ・ 問題発生時の対応 ・ 関連事業者との協力 ・ 動作確認・テスト結果の報告 **【2.案件の種類・特性によって追記すべき要求要件】** ・ 既設のシステムとの結合が必要になる案件の場合には、実施すべきテスト（及び支援内容）、アプリケーション ・ 運用事業者等との役割分担については明確に記載
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○動作・接続確認試験 (1) 本仕様書を満たすことを確認するため、本システム用機器等の動作確認試験及び接続確認試験を実施すること (2) 受注者は、本システム用機器導入及び当省が別途調達する○○システム移行改修後、本システムに係るシステムテストを改修業者と協力して行うこと。システムテストにおいて、本調達に起因する不具合が発見された場合は、原因を分析し正常に作動するまで環境設定等の作業を行うこと。
案件・情報システムの特性等による留意点	接続対象となるシステム、システム規模等により動作検証として実施すべき項目や内容が異なる場合があることから、必要なテスト要件については事前に明確化しておくべきである。 テストに際しては、アプリケーション構築事業者などとの連携が必要になる場合がある。役割分担については明確化しておく必要がある。

セキュリティに関する留意点	—

7. 移行業務

項目	内容
役務内容の概要	現行システムからのデータ、システム、業務等の移行作業（アプリケーションプログラムの変更等を伴わない更新の場合）又は設計・開発事業者が実施する移行作業の支援を実施する。
想定されるインプット（発注者側で用意）	・ 移行データの種類・量及び存在場所の概略 ・ 移行計画書
成果物（受注者側で用意）	・ 移行設計書 ・ 移行データ検証結果報告書
仕様書に記載すべきポイント	受注者がデータ移行を行う場合は、データ受け渡し等の条件について記載する。データ移行をシステム開発事業者などが実施する場合は、移行支援として実施すべき役務要件を記載する。 **【1.基本的に記載すべき要求要件】** ・ 移行対象 ・ 移行作業内容 ・ 移行作業支援内容 ・ 移行作業の前提条件 ・ 移行作業の制約（作業実施可能な時間帯、実施可能な期間、移行方式　など）
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○データ移行要件 受託者は、現行システムが保有するデータの移行作業を実施すること。 (ｱ) 移行データの概略は下記の通り。詳細は、契約締結後、本省より提示する。 （略） (ｲ) 移行実施後、移行されたデータの完全性についてのデータ検証を実施し、その結果を「移行データ検証結果報告書」として報告すること。
案件・情報システムの特性等による留意点	移行業務の実施主体については明確に事前に決めておく必要がある。 受注者が移行支援を行う場合は何処までが支援の範囲となるのか可能な限り明確化しておく必要がある。
セキュリティに関する留意点	―

8. 運用･保守事業者等への情報提供

項目	内容
役務内容の概要	運用・保守等を担当する事業者に機器又はソフトウェアの設定、操作方法に関する情報の提供を行う
想定されるインプット （発注者側で用意）	・ 機器管理情報交換ファイル仕様書
成果物 （受注者側で用意）	・ 機器管理情報 ・ 設定情報 ・ マニュアル
仕様書に記載すべきポイント	運用、保守事業者に機器導入事業者から引き継ぐべき情報を抽出し、その方法について記載する。 **【1.基本的に記載すべき要求要件】** ・ 引き継ぐ情報 ・ 引継ぎ方法
仕様書記載上の例/説明	○引き継ぐ情報 本システムの運用監視および構成管理に必要な機器管理情報および設定情報を文書化し、運用・保守事業者に提供すること。また、運用のためのマニュアルを作成すること。 ○引継ぎ方法 本調達で納入される機器が設置されるまでに、運用・保守事業者に対して操作方法などの説明を行うこと。また、機器の導入後に、運用・保守事業者に対して引継ぎを行うこと。引継ぎにあたっては、確実かつ効果的に操作方法などを伝える工夫を提案すること。
案件・情報システムの特性等による留意点	運用事業者・保守事業者が必要とする情報を不足なく引き継ぐ必要がある。
セキュリティに関する留意点	―

9. 利用者への情報提供･教育

項目	内容
役務内容の概要	一般職員及びシステム担当者に対して、システムの操作方法についての教育を実施する。
想定されるインプット （発注者側で用意）	・ 教育が実施可能な日時・場所 ・ 教育受講対象者数 ・ 想定する教育日程（案）
成果物 （受注者側で用意）	・ 教育スケジュール ・ 各種手順書 ・ テキスト
仕様書に記載すべきポイント	受注者が一般職員及びシステム担当者に操作方法の教育を実施する場合は、対象者・実施方法を記載する。 【1.基本的に記載すべき要求要件】 ・ 教育すべき内容 ・ 実施方法 ・ 実施対象 ・ テキスト
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○教育支援等 動作確認試験後に、本システムの運用上必要な機器等の操作方法等について、担当職員に対して研修を実施すること。 当システムの利用にあたり、○○担当者○○人への教育を予定している。 教育受講予定者の IT レベルは○○ということを考慮して､受託者は、テキストを作成すること。テキストは図等を用い、わかりやすく作成し、職員の了解をとったうえで展開すること。 また、本システムの稼働開始までの期間を考慮し、研修スケジュールを策定すること。研修スケジュールは、予備日を用意すること。
案件・情報システムの特性等による留意点	職員向け、もしくはシステム担当職員向けのシステム等、利用者により IT リテラシ等に差異があることを考慮に入れる必要がある。 最終的な局面（研修・教育の場）で利用者から不満が出る可能性がある事から、各局面（画面イメージ作成時、ある程度システムが完成した時点等）でユーザに対するレビューを計画する必要がある。
セキュリティに関する留意点	―

10. 検収

項目	内容
役務内容の概要	必要な納入物一式を準備の上納入し、府省庁の求める受入試験に対して対応を行う
想定されるインプット（発注者側で用意）	・ 納入物一覧
成果物（受注者側で用意）	・ 納入物として指定された文書一式
仕様書に記載すべきポイント	別途納入期日、納入物品、及び府省庁の設定する受入試験に対応した上で検収とする旨を記載。 **【1.基本的に記載すべき要求要件】** ・ 納入成果物の提出と承認 ・ 受入試験への対応と承認 **【2.案件の種類・特性によって追記すべき要求要件】** ・ 受入試験の項目の設定
仕様書記載上の例/説明	**仕様書に記載する場合の例** 〇納入成果物の提出と承認 受注者は、検収を行うために必要な文書一式を準備の上、承認を得ること。 〇受入試験への対応と承認 受注者は、検収を行うために実施する受入試験について、本省の指示にしたがい、対応すること。
案件・情報システムの特性等による留意点	然るべきタイミングでレビューを設定し、検収時に手戻りが発生することを防ぐ必要がある。
セキュリティに関する留意点	－

6.7.3.納入成果物と提出のタイミング

納入成果物とタイミングを記載すると、下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業内容	納入成果物	納入期限
1. 計画策定	実施計画書	導入作業開始前まで
2. 関係者への事前説明･調整	事前調整･説明会の資料および議事録（支援の場合はドラフト）	各作業の実施前に随時
3. 現地調査･設計	現地調査計画書	現地調査作業開始前まで
	現地調査報告書 施工図面 機器設置レイアウト図 ラック搭載図 配線図 その他各種設計書	導入拠点の工事開始前まで
4. 機器導入･設置作業	ハードウェア、ソフトウェア一式 施工図面･機器設置レイアウト図･ラック搭載図･配線図･その他各種設計書の変更書	仕様書に定める日まで
5. 機器のセットアップ	環境定義書	機器セットアップ後
6. 動作確認･テスト	テスト仕様書	動作確認･テスト開始前まで
	テスト結果報告書 （動作試験報告書）	動作確認･テスト実施後
7. 移行業務	移行設計書	移行作業実施前
	移行データ検証結果報告書	移行作業実施後
8. 運用･保守事業者等への情報提供･教育	機器管理情報 設定情報 マニュアル	導入作業終了日まで
9. 利用者への情報提供･教育	教育スケジュール 各種手順書 テキスト	—
10. 検収	指定された納入物一式	検収日

6.7.4.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載する必要がある。

役務作業	インプット	インプットを提示するタイミング
1.計画策定	スケジュール全体像 役割分担表	入札公示時に調達仕様書・付属資料に記載する
2.関係者への事前説明・調整	各拠点・関連事業者の連絡先 導入対象拠点の一覧 導入対象機器一覧	入札公示時に調達仕様書・付属資料に記載する
3.現地調査・設計	各府省庁で定めるセキュリティガイドライン	Web で開示、又は応札期間中
	施行図面 機器設置レイアウト図 ラック搭載図 配線図 その他各種設計書 （上記に関しては現行のものについて）	応札期間中
4.機器導入・設置作業		
5.機器のセットアップ	ハードウェア要件、ソフトウェア要件、ネットワーク要件、運用保守要件	契約後
6.動作確認・テスト	動作確認項目一覧 他機能群との連携方針等のテスト実施に必要な情報	入札公示時に調達仕様書・付属資料に記載する
7.移行業務	移行データの種類・量及び存在場所の概略 移行計画書	契約後
8.運用・保守事業者等への情報提供・教育	機器管理情報交換ファイル仕様書	入札公示時に調達仕様書・付属資料に記載する
9.利用者への情報提供・教育	教育が実施可能な日時・場所等	入札公示時に調達仕様書・付属資料に記載する
10.検収	納入成果物一覧	入札公示時に調達仕様書・付属資料に記載する

6.7.5.役割分担

分離・分割調達では分離発注の範囲、府省における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表を作成することが必要である。

役割分担表の例

主要業務 ◎：結果責任 ○：実施責任 △：確認	省	運用業者	受託者	開発業者
①計画策定			◎	○
②関係者への事前説明・調整			◎	○
③現地調査・設計			◎	○
④機器導入・設置作業			◎	○
⑤機器のセットアップ			◎	○
⑥動作確認・テスト			◎	○
⑦移行業務			◎	○
⑧運用・保守事業者等への情報提供		△	◎	○
⑨利用者への情報提供・教育			◎	○
⑩検収	◎	△	○	△

6.8.iDC 設備調達付帯作業

6.8.1.調達分野の定義

iDC 設備調達付帯作業とは、各種の機器を受託者が用意する施設内に設置し、回線等ネットワーク環境経由で利用できるようにするとともに、対象システムの運用監視と付随するサービスを実施する事を指す。

役務調達の分類において、運用技術として定義されている箇所に相当し、計画、運用、保守等の役務を対象とする。尚、iDC 設備の機能・サービスに関する要件・仕様については、「5.3 iDC・設備」を参照のこと。

なお、府省庁が提供する建物に、情報システム機器稼働に必要な設備（ラックや冷却装置等）を調達するだけの役務は機器調達に含まれるため、本記載では記述の対象としない。

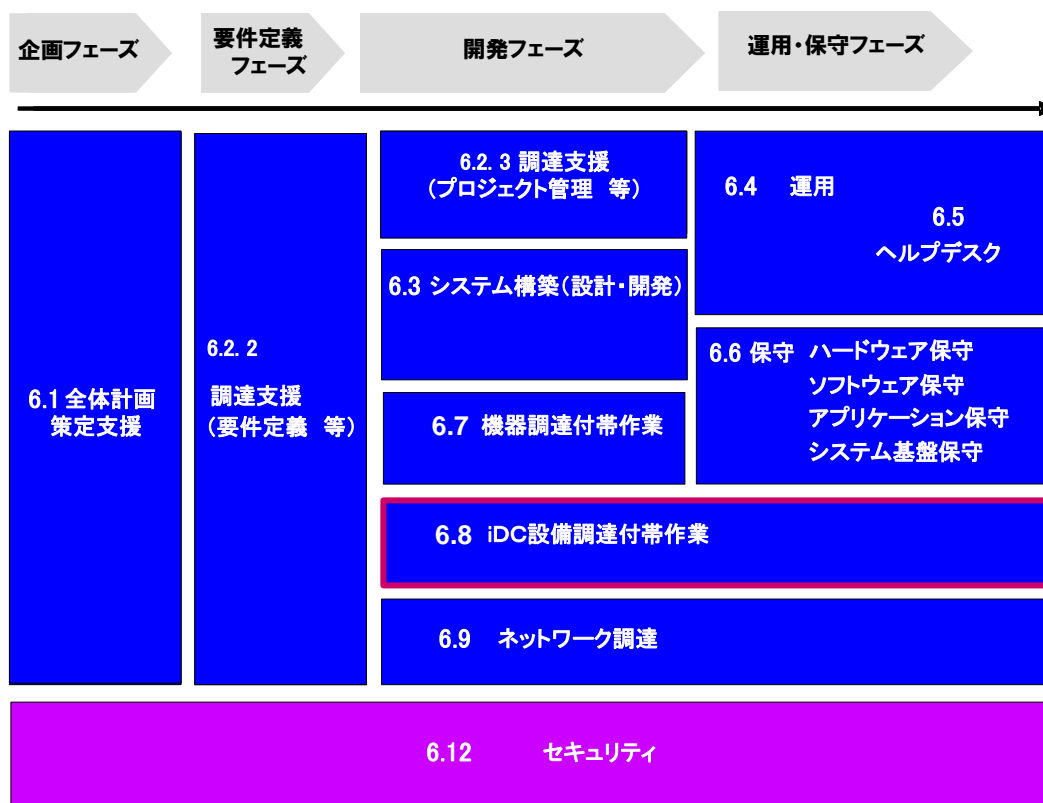



図　6. 8 –1　役務調達の分類における対応箇所

6.8.2.仕様書に記載すべき役務内容

6.8.2.1 代表的な役務の内容

仕様書に記載すべき、役務の内容は下記の通りである。尚、対応する SLCP-2007 [13]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[14]の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整しつつ、適切な項目立てで調達仕様書案を作成することが望ましい。

役務作業	役務作業の概要	共通フレーム 2007 の アクティビティ	総務省 データセンターの安全･信頼性に係る情報開示指針 （第 1 版）における役務項目との対応	調達基本指針に対応する仕様書の章･節（及びそのタイトル）
1. 作業計画	実施計画書作成 調達範囲 作業体制 作業スケジュール等	2.3.1 品質保証プロセス開始の準備	62. ～68. 入退館管理等（建物要件記載）	2 章（4）、(5) 4 章、5 章、6 章
2. 作業実施	データセンター作業 回線関連作業（必要に応じて）	3.2.2 環境の構築	―	10 章、11 章、12 章､5 章(5)
3. 運用･保守開始準備	システム運用監視手順書の作成 監視手順書 アタック状況監視手順書 セキュリティ診断手順書 各種報告書書式 各種管理台帳書式 ＳＬＡに関する役務作業要件	3.2.1 （環境整備）プロセス開始の準備	99. SLA	
4. 運用･保守（日次）	日次作業（稼働状況管理､保全管理､報告関連） 日次報告書作成	1.7.4.1 システムの運用 1.7.4.2 運用監視及び運用データの収集、問題の識別､記録及び解決、運用環境の改善 1.7.4.3 問題の識別及び改善 1.7.4.4 運用環境の改善 1.7.7 システム運用の評価 1.8.2 問題把握及び修正分析 1.8.3 修正の実施	60. 24 時間×7 日間/週監視体制 105. ～109. サービス通知･報告 110. ～112. 支援サービス	
5. 運用･保守（週次）	週次作業（データベースバックアップ等） 週次報告書作成			
6. 運用･保守（月次）	月次作業（セキュリティ診断等） 月次報告書作成			
7. 運用･保守（非定常）	非定常に発生する作業についての以下の役務作業 作業内容 報告書作成		69. ～70. 媒体の保管	

[13] 独立行政法人 情報処理推進機構 共通フレーム 2007
ソフトウェアライフサイクルプロセス SLCP-JCF 2007

[14] 総務省 情報システムに関わる政府調達の基本指針 2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

6.8.2.2.各役務内容に関する説明及び仕様書上の記載例

1. 作業計画

項目	内容
役務内容の概要	導入作業（データセンタ設備の調整、回線引き込み、機器設置等）の実施計画書を作成する。
想定されるインプット（発注者側で用意）	データセンタ設置及び運用管理対象機器一覧 設置場所要件 システム構築スケジュール
成果物（受注者側で用意）	実施計画書
仕様書に記載すべきポイント	実施計画立案の要求事項を記載する。 **【1.基本的に記載すべき要求要件】** ・ 調達範囲 ・ 作業実施体制 ・ 作業スケジュール等
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○調達範囲 情報システム化の目的は、○○省の情報システムのサーバ機器類を設置して、○○省の機器類を安全に稼動させるための電源、空調、耐震、物理的侵入の防止等の専門的なサービスを受けるものである。なお、本件の調達範囲は、機器設置に伴う電源設備の準備、機器の耐震固定作業、機器の物理的なセキュリティ対策、設置場所での運用業務とし、以下の要件は含まれない。 ①○○省が利用するサーバ機器類の物品調達とこれに付随する設定作業 ②○○省が利用するサーバ機器類の稼動する情報システムの稼動監視作業 ○作業実施体制 本項目に関する要件は、次のとおりである。 ①調達事業者は、本件を遂行する実施体制を整えること。 ②実施体制は、各チームの役割、作業分担、編成時期等を明確にすること。 ③本作業の作業責任者は、プロジェクトマネージャ、PMP（Project Management Professional）等のプロジェクト管理関連資格又はそれに準ずる知識を有すること。尚、必要とされる資格・知識に関しては、「総務省 情報システムに関わる政府調達の基本

	指針」に従う。 ④本仕様書に定める作業実施要件から必要な項目を洗い出し、WBS（Work Breakdown Structure）を作成し、作業工程間の順序関係や依存関係を明確にして必要作業量に基づいたスケジュール・組織要員計画書を作成すること。WBS は、プロジェクト全体を詳細な作業に分割したことを示す図表のことである。 ○作業スケジュール(委託作業実施のスケジュール) ①平成○年○月○日：データセンタ設備の準備完了 (機器設置予定) ②平成○年○月○日：テストの運用開始 ③平成○年○月○日：本番の運用開始 ④平成○年○月○日：本契約終了
案件・情報システムの特性等による留意点	①調達範囲は、システムごとに異なるため、インターネット回線接続や専用線が不要である場合も想定される。 ②「仕様書記載上の例/説明」は、運用開始後の監視業務が調達対象となっていないが、設備および開始に向けた作業のみを調達する場合も想定される。 ③全般的な要件（要員スキル等）の記載にあたって、複数の役務を調達するような場合には記述が複数回出現することは効率面で望ましくないため、全体的にまとめて記述する等の工夫をすることも検討すること。 委託スケジュールについては、データセンタ側の設備準備の観点から、提示するシステム構築スケジュールに機器設置予定日が記載されていることが望ましい。
セキュリティに関する留意点	―

2．作業実施

項目	内容
役務内容の概要	データセンタ作業（設備の準備、機器設置）を行う。また、必要に応じて回線引き込み等関連作業を行う。
想定されるインプット （発注者側で用意）	対象機器一覧，ネットワーク図 （設置機器情報詳細，iDC に引込む回線の種別や接続先詳細）
成果物 （受注者側で用意）	作業完了報告書
仕様書に記載すべきポイント	作業実施の要件を記述する。 **【1.基本的に記載すべき要求要件】** ・　データセンタ設備準備・調整作業 ・　機器設置作業支援（ケーブル結線等） **【2.必要に応じて記載すべき要求要件】** ・　回線関連作業実施要件
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○データセンタ設備準備・調整作業 (1)　機能構成 ５．３章に示す要件のうち、本件で調達するのは、「iDC・設備」の「立地条件、施設条件、マシンルーム条件、電源･空調条件、セキュリティ条件、運用条件」である。これ以外の箇所は本件とは別の調達となる。 (2)　規模要件 ○○省が設置を要請する台数は、次のとおりである。 サーバ等情報システム機器　：__台 ルータ及びスイッチ類等ネットワーク機器　：__台 ラック　：__台 また、運用作業者__名（又は__㎡）のオペレーションルームも調達する（オペレーションルームとサーバとのネットワーク配線も調達範囲に含まれる）。 運用端末設置机　__台 鍵付キャビネ　__台 (3)　調達作業 ①設置レイアウト（ラック搭載含む）設計 データセンタへ設置する情報システム機器の設置場所についてデータセンタ内のレイアウト設計を実施する。データセンタ所

	有のラックを借用する場合は、提示した機器一覧に基づきラック搭載図を作成する。 ②電源接続設計 電源接続に関して割り当てブレーカ等を明確にした電源結線・接続図を作成する。電源冗長化が必要な場合は分電盤を別系統で割り当てるなど、分電盤を含めた冗長化を考慮すること。 ③設備準備 レイアウト・電源接続設計結果に基づいてラック設置に伴う耐震固定作業・電源準備作業等の設備準備を行う。 (4) 作業実施要件 ①WBSをベースとした管理手法を用いてプロジェクト管理を行うこと。 ②調達事業者は本作業内容を鑑みた上での進捗管理方法を○○省の担当者に提案すること。調達事業者は、○○省の担当者が確認した進捗管理方法に従って本作業を推進・管理すること。 ③定期的な進捗報告会を開催し、作業状況（計画、実績及びその差異）等を報告すること。 ④○○省の担当者との打合せは日本語で行い、打合せ資料、納品ドキュメントは日本語で記載すること。 ⑤実施体制を変更する場合、その旨を○○省の担当者に報告して確認を得ること。 ○機器設置作業支援（ケーブル結線等） ①機器搬入立会い 機器設置時の搬入路の確保、サーバルーム内設置場所への誘導を実施する。 ②電源結線支援 電源接続に関して分電盤と電源タップの結線及びラック内電源タップと機器電源ケーブルの接続について、設置業者への指示・管理を行う。 ③各種ケーブル敷設・結線支援 LANケーブルやファイバーケーブル、外部接続用回線等の敷設に伴う保護用ダクト・トレイ等を準備する。 ○回線関連作業実施要件(基本要件) ①回線の終端装置は受注者が提供すること。ルータやスイッチ類は別途調達するハードウェア事業者が持ち込み、設置する。 ②○○○庁舎への回線引き込みに関して、配管、電源工事は調達

	範囲とする。 ③回線利用開始は、平成○年○月○日とする。
案件・情報システムの特性等による留意点	①導入作業役務については、回線の有無等によって変化するものと想定される。また、記述についても、上記のように作業要件を規定する場合のほか、技術要件以外の要素は記述せず、受注者に作業項目定義を任せることも選択肢のひとつである。 ②電源接続設計において、電源の冗長化が必要な機器については対象機器一覧に明記し、必ず異なる分電盤から受電されるように指示することが必要である。 ③ケーブル敷設については、電源ケーブルや通信関連のケーブルが混在する環境では、相互干渉によって通信途絶などの影響が出る可能性があるため、干渉防止のための配管やトレイを準備することを要求しておくことが必要である。 ④○○○庁舎への回線引き込みに関する配管、電源工事は、庁舎設置場所の状況（契約他）により調達範囲とするか否か判断する。
セキュリティに関する留意点	―

3．運用･保守開始準備

項目	内容
役務内容の概要	システム運用監視を行う際の、運用事業者向け作業手順書を作成する。
想定されるインプット（発注者側で用意）	システム運用監視項目一覧
成果物（受注者側で用意）	システム運用監視手順書 各種報告書書式 連絡体制図
仕様書に記載すべきポイント	新規に構築・拡張したネットワークと既存ネットワークを接続し、移行を実施又は支援する作業について、その要件ならびに計画立案に必要な項目等を記載する。 **【1.基本的に記載すべき要求要件】** ・ システム運用監視手順書の作成 ・ 各種報告項目・書式の作成 ・ 各種管理台帳等の作成 ・ SLA(Service Level Agreement)に関する役務作業
仕様書記載上の例/説明	**仕様書に記載する場合の説明** ○運用マニュアルの作成 システムの開発業者/機器納入業者/システム運用支援業者と連携し、調達事業者が「運用マニュアル」を作成する。 作成する「運用マニュアル」の内訳は以下のとおり。 ①監視環境操作手順書 システム運用監視環境の操作方法、監視項目一覧で示す項目（ノード監視、プロセス監視等）の各々の監視手順を記載する。記載にあたっては監視画面、付帯する機器（パトライト等）等監視に関わる環境を網羅する。 なお、異常検知時の連絡等対応方法や監視項目等の設定変更方法に関しても記載する。 ○各種報告項目、書式類の作成 ○○省と連携し、システム運用監視・アタック状況監視等の作業結果について、○○省への報告を行う際の報告内容の決定と報告書式の作成を行う。また、非定常作業の依頼等を受け付ける際の依頼書式についても同様に連携の上、作成する。 ①報告内容の決定

	システム運用監視項目に基づき、報告項目(日時、サーバ名、発生事象等)・報告時期(日次、月次等)・提出方法(印刷物・メールなどの電子データ等)・提出先などを決定する。 ②各種書式類の作成 非定常作業に関する依頼書式及び①にて決定した報告項目を提出する際の報告書書式を作成する。作成する報告書は概ね下記項目があるが、監視項目によって詳細化する。 （ア）非定常作業依頼書兼報告書 （イ）システム運用日次報告書（ウ）システム運用週次報告書 （エ）アタック状況報告書（月次） （オ）インシデント(異常)報告書 （カ）システム運用月次報告書 （キ）セキュリティ診断報告書（月次） ○各種管理台帳等の作成 ○○省と連携し、iDC 設備に設置・運用・管理される内容について、管理台帳を作成する。 ①各種管理台帳 （ア）ハードウェア構成管理台帳 （イ）ネットワーク引き込み管理台帳 （ウ）ドキュメント管理台帳 （エ）バックアップメディア管理台帳 （オ）連絡体制図 （カ）大規模災害発生時の対策方針・連絡体制 ○SLA に関する役務作業 SLA 項目に対する達成状況を月単位で評価し、それらを 3 ヶ月毎に実施する「サービスレベル報告会」において、3 ヶ月分を集計した結果を報告する。
案件・情報システムの特性等による留意点	①既存のネットワークやデータセンタに収容されている既存の府省システムが存在しない場合は、計画書作成にあたり既存ネットワークやシステムを担当する他事業者との連携は必要とならないと思われるが、一方で多くの調達では既存システムが存在することから上記事例を引用している。 ②運用マニュアルについては、インターネット接続やファイアーウォール等について iDC 事業者保有の設備を利用する場合を前提として記載しているが、個別にネットワーク事業者等の関連事業者が準備する場合は、委託項目に基づいて項目を定義する。

	③大規模災害発生時のiDC事業者の対応方針と○○省担当者との連絡体制を明確にする。データセンタを複数箇所保有し、ディザスタリカバリセンターを構成する場合は、プライマリセンター･バックアップセンター間の連絡方法についても定義する必要がある。 ③SLA に関する評価項目・報告･見直しサイクル等 SLM(Service Level Management)については、項目数や頻度を高めた場合、SLM に必要となるコストが増大するため、「仕様書記載上の例/説明」では 3 ヵ月毎としているが、システムの重要度等を考慮し決定すること。
セキュリティに関する留意点	

4．運用･保守(日次)

項目	内容
役務内容の概要	運用・保守について、毎日の業務として実施および報告すべき作業である。
想定されるインプット （発注者側で用意)	運用マニュアル セキュリティ状況監視手順書
成果物 （受注者側で用意)	システム運用日次報告書 インシデント(異常)報告書（発生時のみ)
仕様書に記載すべきポイント	運用・保守実施項目、要件等を記載する。 **【1.基本的に記載すべき要求要件】** ・日次作業 （設備維持管理、システム稼働状況監視、保全管理、報告関連） ・システム運用日次報告書作成
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○日次作業 ①設備維持管理 iDC 設備として提供する電源・空調設備、各種災害検知装置(煙センサー等)、監視カメラ等の監視を行う。 入退室に関するセキュリティ装置の維持管理、来場者の受付・入退室対応を実施する。 ②稼働状況管理 「３．運用・保守開始準備」で規程した監視項目について運用マニュアルに従って監視をする。 （監視項目例） システム死活監視 プロセス監視 イベント・メッセージ監視 キャパシティ監視 ～以下省略 ③保全管理 定期巡回によりランプ（LED(状態表示ランプ)、インジケータ表示、機器のステータス表示等）の目視確認等を行い、機器の状態を監視する。 ④報告関連 日次作業において障害を発見した場合や、手順外の状況となるなどの問題を検知した場合、指定された連絡･対応方式に基づき

	報告を実施する。 ○システム運用日次報告書作成 上記①、②の実施状況についてシステム運用日次報告書に記録する。
案件・情報システムの特性等による留意点	①データセンタに収容されているシステムの重要性等により、日報等が必要と想定されない場合は本項目は記載しないこともある。ただし、月次での報告は最低限必要であると考えられる。
セキュリティに関する留意点	セキュリティ監視 セキュリティ状況監視（ファイアーウォールのログの精査、不正侵入の監視等）ならびに監視結果を定期的に府省担当者への報告を行うこと。

5. 運用･保守(週次)

項目	内容
役務内容の概要	運用・保守について、週次の業務として実施および報告すべき作業である。 　週次作業（データベースバックアップ等） 　週次報告書作成
想定されるインプット （発注者側で用意）	運用マニュアル
成果物 （受注者側で用意）	システム運用週次報告書
仕様書に記載すべきポイント	運用・保守実施項目、要件等を記載する。 **【1.基本的に記載すべき要求要件】** ・週次作業 ・システム運用週次報告書作成
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○週次作業 　週次で実施される全データベースバックアップのジョブ成否確認を行い、テープクリーニング及びメディア交換を実施する。 　週次作業において障害を発見した場合や、手順外の状況となるなどの問題を検知した場合、指定された連絡･対応方式に基づき報告を実施する。 ○システム運用週次報告書作成 　上記週次作業の実施状況について、システム運用週次報告書を作成する。
案件・情報システムの特性等による留意点	①データセンタに収容されているシステムの重要性等により、週次での作業や報告等が必要と想定されない場合は本項目は記載しないこともある。ただし、月次での報告は最低限必要であると考えられる。
セキュリティに関する留意点	－

6．運用･保守(月次)

項目	内容
役務内容の概要	運用・保守について、月次の業務として実施および報告すべき作業である。 月次作業（セキュリティ診断等） 月次報告書作成
想定されるインプット （発注者側で用意）	運用マニュアル セキュリティ診断手順書
成果物 （受注者側で用意）	システム運用月次報告書 セキュリティ診断報告書
仕様書に記載すべきポイント	運用・保守実施項目、要件等を記載する。 **【1.基本的に記載すべき要求要件】** ・月次作業 ・月次報告書作成
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○月次作業(セキュリティ診断) 月に１回、「３．運用・保守開始準備」で作成したセキュリティ診断手順書に基づきセキュリティ診断を実施する。診断結果（脆弱性に関する説明、影響、対応方法）を取りまとめ「セキュリティ診断報告書」として報告及び提出すること。 ○システム運用月次報告書作成 上記月次作業の結果についてセキュリティ診断報告書を作成する。また、当月のシステム運用・保守作業実施状況・インシデント発生状況の集計などについて月単位で纏め、システム運用月次報告書を作成する。
案件・情報システムの特性等による留意点	①SLA についての項目は原則的に規定すべきと想定しているが、システムの重要性等を鑑み、SLA を規定しない場合は SLA 実績報告は行わないこととなる。
セキュリティに関する留意点	セキュリティ診断と報告 定期的に脆弱性の診断を行い、その結果（状況、影響、対応方法）を府省担当者に報告すること

7．運用･保守(非定常)

項目	内容
役務内容の概要	運用・保守について、非定常の業務として実施および報告すべき作業である。
想定されるインプット （発注者側で用意）	運用マニュアル 非定常作業依頼書兼報告書（依頼部分）
成果物 （受注者側で用意）	非定常作業依頼書兼報告書（報告部分） その他作業結果報告書（様式等規定なし）
仕様書に記載すべきポイント	運用・保守実施項目、要件等を記載する。 **【1.基本的に記載すべき要求要件】** ・作業内容 ・報告書作成
仕様書記載上の例/説明	**仕様書に記載する場合の例** ○作業内容 （1）保全管理 ①定期保守対応 設置される機器等についての定期保守対応を行う際の、ＳＥ／ＣＥの引き込み、立会い、作業前後での必要作業の実施（サーバ停止・再起動等)、保守作業完了の確認等を実施する。 ②障害対応 障害発生時のラップ状態確認・監視状況の報告、ログデータの採取等を実施する。 （2）ストレージ管理 システムの変更や保守・改変作業後のシステムフルバックアップ作業を実施する。 （3）物品管理 ①ハードウェア管理 ハードウェアの追加･変更が発生した場合の受入れ作業･管理台帳の更新を実施する。 ②媒体管理 媒体の破損・劣化による交換が発生した際の、業者からの新品媒体の受け取り、新品媒体への交換、管理台帳の更新を実施する。 （4）その他 ①データセンタ来場者対応（サーバルームへの引き入れ等)

	府省担当者や開発事業者等他事業者などの来場時の引き入れ対応（ラック設置場所への案内等）を実施する。 ②各種物品（消耗品等）の搬送業者との授受対応 府省担当者や関連事業者、システムに関連する外部取引業者等から物品を受け取る、あるいは物品の送付を行う際の対応を実施する。 ③監査対応 外部団体を含む各種監査において iDC が監査対象となった際の監査受け入れ・質問表への回答等を実施する。 ④機器撤去対応 設置機器・ラックの撤去・データセンタ移転等が発生する場合は、ラックの固定解除・電源の引き戻し、運用手順の引継ぎを行い、機器調達ベンダー等関連業者と連携して対応を実施する。 （５）照会等対応 ランプ状態確認やハードウェア設置状況、データセンタ設備に関する問合せ等、iDC 設備・運用に関する問い合わせ・情報提供依頼に対する対応を実施する。 （６）報告書作成 非定常作業依頼書兼報告書に基づく作業結果について非定常作業依頼書兼報告書を作成する。その他作業を実施した場合も、作業結果等について報告書（様式等規定なし）を作成する。
案件・情報システムの特性等による留意点	①突発事項や府省からの臨時の要請により、何らかの非定常な作業を行うケースはあるものと想定されるが、その内容は運用・保守作業項目によって適切なものとする必要があり、またシステム運用の特性から定常作業のみで実施可能と判断される場合は規定しないこともありうる。 ②監査対応について、定期的な監査が決まっている場合は、その内容、頻度を提示する。
セキュリティに関する留意点	－

6.8.3.納入成果物と提出のタイミング

納入成果物とタイミングを纏めると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即して記載をする必要がある。

役務	納入成果物	納入期限
1. 作業計画	実施計画書	契約後、作業開始の5営業日前まで
2. 作業実施	作業完了報告書	作業完了後の5営業日以内
3. 運用･保守開始準備	システム運用監視手順書 各種連絡書書式 連絡体制図	運用前の文書策定時（運用訓練開始前迄）
4. 運用･保守（日次）	システム運用日次報告書 インシデント（異常）報告書（発生時のみ）	運用開始後毎日
5. 運用･保守（週次）	システム運用週次報告書	運用開始後週次
6. 運用･保守（月次）	システム運用月次報告書 セキュリティ診断報告書	運用開始後月次
7. 運用･保守（非定常）	非定常作業依頼書兼報告書(依頼部分)	作業完了後の5営業日以内

6.8.4.想定されるインプット

受注者(もしくは提案者)に対して事前に提示すべきインプットとタイミングを記載すると下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即して記載をする必要がある。

役務	インプット	インプットを提示するタイミング
1. 作業計画	データセンタ設置及び運用管理対象機器一覧	入札公示時に調達仕様書･付属資料に記載する
	設置場所要件	入札公示時に調達仕様書･付属資料に記載する
	システム構築スケジュール	入札公示時に調達仕様書･付属資料に記載する
2. 作業実施	対象機器一覧，ネットワーク図	入札公示時に調達仕様書･付属資料に記載する
3. 運用･保守開始準備	システム運用監視項目一覧	入札公示時に調達仕様書･付属資料に記載する
4. 運用･保守（日次）	運用マニュアル セキュリティ状況監視手順書	―
5. 運用･保守（週次）	運用マニュアル	―
6. 運用･保守（月次）	運用マニュアル セキュリティ診断手順書	―
7. 運用･保守(非定常)	非定常作業依頼書兼報告書（報告部分）	―

iDC設備におけるサービスレベル設定案の例を以下に示す。項目・数値は参考であり、個々の案件・システムの重要度等に応じて決定されるべきものである。委託者(○○府省)と提供者(iDC 事業者)双方による合意の結果としてSLAを設定することで提供されるサービス品質の水準を明確に規定し、SLMによってサービ

スレベルの維持・管理を行う。SLA には目標保障型と努力目標型の 2 種類があり、項目ごとに取り決める。

iDC 設備におけるサービスレベル設定例を以下に示す。項目・数値は参考値であり、個々の案件・システムの重要度等に応じて決定されるべきものである。

項番	分類	サービスレベル項目	規定内容	単位	サービスレベル設定例
1-1	可用性	サービス時間帯	iDC設備を提供する時間帯	時間帯	サービス時間帯(サービスの種別により設定)を定義する。 サービス種別例: ・電力供給 ・運用サービス ・稼動監視 時間帯設定例: ・24 時間×7 日間／週 ・24 時間×7 日間／週 (計画停止/定期保守を除く) ・9-17 時 サービス停止の連絡(役務時間内に停止が生じる場合、計画停止時間は提供者が個々に設定するが、計画停止の事前連絡を規定。)
1-2		サービス稼働率	稼働率(電力供給) ー 通電時間／サービス時間	稼働率	設置機器への電力供給の継続を管理する。99.8%以上の可用性など。 ただし、冗長化電源を採用している場合は、供給断と判断する定義を設定しておく必要がある。
1-3			稼働率(設置環境) ー 管理範囲内での提供時間／サービス時間	稼働率	サーバルーム温湿度の管理設定値(24℃±4℃)を設け、その範囲内にコントロールする事とし、管理範囲内で運営されているかどうかを管理する。 設定例: 管理上限値と下限値に 99.5%以上の確率でコントロールされていること
1-4			稼働率(ネットワーク) ー ネットワーク稼働時間／ネットワーク稼動予定時間(サービス時間)	稼働率	iDC設備として調達したネットワークに関する可用性を定義する。99.9%以上の可用性など
1-5			稼働率(監視環境) ー 監視サービス提供時間／監視サービス提供予定時間(サービス時間)	稼働率	iDC設備として調達した各種監視環境に関するシステム稼働率を定義する。 99.5%以上の可用性など。
2-1	信頼性	オペレータ要員数	該当システムの運用に携わる要員数	要員数	調達対象システム専用のオペレーション体制を構築する場合は、要員数について定義する。
2-1		正確性	オペレータ1人あたりのミス率(運用手順書外の操作)	ミス率(%)	運用手順書記載の内容について誤操作、誤入力等を行った回数について定義する。回数の定義ではなく、ミス率とする場合は、母数の設定に注意する必要がある。
2-3		オペレータ要員	オペレータ教育回数	教育受講回数	ISO関連やセキュリティポリシー等を含むオペレータ教育の実施について、毎6ヶ月ごとに 8 時間などの教育回数を定義する。

項番	分類	サービスレベル項目	規定内容	単位	サービスレベル設定例
2-4	信頼性	障害通知プロセス・通知時間	障害発生時の連絡プロセス（通知先／方法／経路）の設定と、連絡プロセスに基づき設定された通知先に通知するまでの時間 ・通知方法例 　－　電話、メール、ホームページ ・通知先例 　－　サービスの提供を受ける顧客 　－　サービスのオーナー(サービスをアウトソースしているケース）	有無 時間	・指定された緊急連絡先にメール/電話で連絡し、あわせてホームページで通知 ・通知先に応じた通知時間の設定 ・営業時間内／外のサービスレベルに応じた設定 これら3点を考慮したSLAの設定を実施する。 想定されるケースとして次のようなものがある。 ケース1 サービスの提供を受けている顧客、あるいはサービスのオーナーに電話あるいはメールによる営業時間内の障害通知（例：自動通知システムの場合1分以内。連絡に人を介する場合5分以内） ケース2 サービスの提供を受けている顧客、あるいはサービスのオーナーに電話あるいはメールによる営業時間外の障害通知（例：自動通知システムの場合1分以内、連絡に人を介する場合10分以内） ケース3 サービスの提供を受けている顧客に対するホームページでの障害発生報告、および掲載目標時間（発生時間、回復見込み時間などホームページには障害発生から30分以内に掲載）
2-5		障害監視間隔	障害インシデントを収集／集計する時間間隔 （機器の動作状況の確認頻度）	時間	営業時間内／外で異なる設定を行う場合がある。 1 分以内（基幹業務） 15 分（上記以外）

6.8.5.役割分担

ハードウェア保守事業者と府省庁、その他業務の調達事業者との役割分担について、本項でひとつの例を紹介する。

分離・分割調達では、分離発注の範囲、府省庁における方針に即して、調達する役務、関係する調達と当該調達との役割分担を設定し、入札公示時に提示することが重要である。

調達検討にあたっては、調達全体で実現される役務を明らかにし、分割された調達の役務・役割にヌケ・モレがないことが当事者間で合意できるよう、明確な役割分担と役務を設定し、役割分担表で提示することが必要である。

（○○省　「データセンタ借入等 一式」仕様書、平成 22 年 4 月）

○各事業者との役割分担等

（1）　技術支援及び情報提供等

イ．　進捗等把握のための資料提出

受注者は、指摘や進捗等把握のための資料提出依頼等があった場合は、
○○省と協議の上、内容に沿って適切な対応を行うこと。

ロ．　納入物の適正な使用に関する助言

受注者は、本調達における納入物の適正かつ効率的な使用に関する
質問に対する回答、助言等を行うこと。

ハ．　システム監査への対応支援

本調達における納入物に関するシステム監査等が実施される場合は、
受注者は積極的に技術支援及び情報提供等を行うこと。

（2）　関係者との調整

イ．　関連事業者との調整

受注者は、本システムの設計・開発・テスト、移行及び稼働開始に係る受注者
（以下、「システム構築事業者」という。）、本システムの稼働後における
運用監視管理に係る受注者（以下、「運用事業者」という。）、本システムに係る
他の調達案件の受注者（○○サブシステムサーバ保守事業者、その他
ハードウェア保守事業者。以下、「関連事業者」という。）への依頼や調整等に
ついて、○○省の承認を得て実施すること。

ロ．　外部関連事業者との調整

受注者は、本システムに関係する他のシステムに関わる事業者（現行システム
運用事業者等。以下、「外部関連事業者」という。）への依頼や調整等について
は、○○省と協議すること。また、必要となる調整作業を支援すること。

（３）役割分担例

導入作業（１．作業計画～３．運用･保守開始準備）における作業分担と本番稼動（４．運用保守（日次）～６．運用保守（非定常））、撤去作業（７．撤去作業）における作業分担の一例を示す。

イ．　導入作業

○：主担当、△：支援、助言

作業項目	主管課	保守事業者	運用事業者	ﾈｯﾄﾜｰｸ事業者	iDC 事業者	ｼｽﾃﾑ構築事業者	機器調達事業者
インプット情報の整備･提示	○	△	△	△			△
iDC 設備に関する WBS 作成					○		
定例報告会	△				○		
ｻｰﾊﾞﾙｰﾑ設置ﾚｲｱｳﾄ作成					○		
ﾗｯｸ搭載図の作成　(※1)					○		
電源接続図の作成					○		
ﾗｯｸ耐震固定作業(標準ﾗｯｸ準備　(※1))					○		
電源準備作業					○		
機器搬入作業							○
搬入作業立会い(設置場所指示他)					○		
各種ｹｰﾌﾞﾙ関連設備準備（※2)					○		
機器設置							○
ｹｰﾌﾞﾙ結線作業				○			○
結線作業支援(接続先指示､FA 床下作業等)					○		
運用監視環境の準備(※3)					○		
運用監視手順書の作成（※3)					○		
運用受入れ訓練			△		○		
受入れ訓練の指導						○	○

※１：iDC 事業者提供ラックを使用する場合の分担を記載しています。
　　機器調達事業者にてラックも準備する場合は、調達事業者にて作成･準備する。

※２：各種ｹｰﾌﾞﾙ関連設備とは、メタル回線用ローゼットの準備や光回線用保護ダクト、
　　LAN ケーブル等の保護ダクト(又はトレイ)等を指す。

※３：iDC の運用監視環境を利用する場合の作業分担を示す。システム開発ベンダ等
　　関連事業者にて監視環境を構築する場合は、別途作業分担を詳細化する必要がある。

ロ．運用作業

〇：主担当、△：支援、助言

作業項目	主管課	保守事業者	運用事業者	ﾍﾙﾌﾟﾃﾞｽｸ事業者	ﾈｯﾄﾜｰｸ事業者	iDC事業者	機器調達事業者
インプット情報の整備･提示	〇	△	△		△		△
運用作業(日次･週次･月次･非定常) ※オンサイト業務			△			〇	
運用作業			〇			△	
報告書作成						〇	
障害の検知･通報		△	△	△	△	〇	
障害対策の実施		〇	〇	〇	〇		
保守ベンダの来場対応						〇	
媒体の管理						〇	
設備(電源･空調等)の維持管理						〇	
サーバルーム監視 ※監視カメラ、入退室装置等						〇	
サーバルームでの異常通報	△					〇	
利用者からの問い合わせ				〇			

6.9.ネットワーク調達

6.9.1.調達分野の定義

ネットワーク調達における役務とは、①(ネットワーク構築に係わる役務)LAN、WAN 等のネットワーク構築に関連する役務、もしくは②(通信サービス調達に係わる役務)WAN 等の広域ネットワークサービスやインターネット接続サービス等のサービスの調達に係る役務を指す。

ネットワーク構築もネットワークサービス調達も技術ドメインから見た調達パターンにおいては、WAN 設計・構築、省内 LAN 設計・構築として定義されている箇所に相当し、計画、設計、施工、運用、保守等の役務を対象とする。一方、現実の調達においてはネットワークの調達とグループウェアやファイル共有アプリケーション等のサーバおよびソフトウェア調達が同時に行われる事もしばしば見られるが、本記載ではこれらのアプリケーションに係る調達は対象としない。

図 6.9-1 役務調達の分類における対応箇所

6.9.2.ネットワークの構築に係る役務

6.9.2.1.仕様書に記載すべき役務内容

6.9.2.1.1.代表的な役務の内容

仕様書に記載すべき役務の内容は、下記の通りである。尚、対応する SLCP-2007 [15]のアクティビティを併記する。実際の調達に際しては、記載項目にヌケ・モレが無い様、SLCP のアクティビティとの対応状況をチェックすることが望ましい。また、併せて調達基本指針[16]の項目との対応も記載している。実際の仕様書の作成にあたっては、府省全体管理組織と調整して必要な項目の見直しを行い、調達仕様書案を作成することが望ましい。

（1）構築を伴うネットワーク調達を行う場合の役務（省内 LAN 構築や WAN の構築、接続など）

役務	役務の概要	共通フレーム 2007 の アクティビティ	調達基本指針に対応する仕様書の章・節（及びそのタイトル）
1. 設計・開発計画	業務・システム最適化指針（ガイドライン）における「設計・開発段階計画」に相当するものの案を作成 設計・開発実施体制と役割、詳細な作業及びスケジュールの作成	1.6.1 プロセス開始の準備	2章（4）、（5） 4章、5章、6章、7章、8章、9章、10章、11章、12章、13章
2. 設計・開発	ネットワークの設計、ならびに開発・施工・単体テスト （ネットワーク機器、装置のハードウェア調達はこれに含まない）	1.6.1 プロセス開始の準備 1.6.3 システム方式設計 3.2.2 環境の構築	
3. 移行計画	新たに構築したネットワークへ現利用者を移行するために必要な作業の計画を立案	1.7.3.2 移行計画の文書化と検証 1.7.3.3 関係者全員への移行計画等の通知	2章（4）、（5） 4章、5章、6章、7章、8章、9章、10章、11章、12章(2)、(4) 13章
4. テストと移行判定支援	新ネットワークが設計どおり動作することを確認するため、システムを利用者に供する前に各種のテストを実施	1.6.13 ソフトウェア受け入れ支援 1.7.1.8 運用テスト計画の策定 1.7.2 運用テスト	
5. 移行	移行を実施	1.7.3.5 関係者全員への移行の通知 1.7.3.6 移行評価のためのレビュー	
6. 運用・保守計画	運用・保守のための体制づくりと運用設計、ドキュメント整理	1.7.1.3 問題管理手続の確立	2章（4）、（5） 5章（5）、6章、7章、

15 独立行政法人 情報処理推進機構 共通フレーム 2007
ソフトウェアライフサイクルプロセス SLCP-JCF 2007

16 総務省 情報システムに関わる政府調達の基本指針 2007 年 3 月
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070301_5_bs2.pdf

役務	役務の概要	共通フレーム2007の アクティビティ	調達基本指針に対応する仕様書の章･節 （及びそのタイトル）
		1.7.1.4 システム運用に係る事前調整、作業手順の確立 1.7.1.8 業務運用に係わる作業手順の確立 1.8.1.2 計画及び手続きの作成	8章、9章、10章、11章、12章(3)、(4) 13章
7.運用･保守業務	運用･保守計画の結果を受けて、運用･保守の実施及び運用状況の報告	1.7.4 システム運用 1.7.4.1 システムの運用 1.7.4.2 運用監視及び運用データの収集、問題の識別、記録及び解決、運用環境の改善 17.4.3 問題の識別及び改善 1.7.4.4 運用環境の改善 1.7.7 システム運用の評価 1.8.2 問題把握及び修正分析	

6.9.2.1.2.各役務内容に関する説明及び仕様書上の記載例

1. 設計･開発計画

項目	内容
役務の概要	業務・システム最適化指針（ガイドライン）における｢設計・開発段階計画｣に相当するものの作成を支援する。
想定されるインプット （発注者側で用意）	・ 開発スケジュール ・ インタビュー等に基づく府省の意見 ・ 府省セキュリティポリシー ・ 導入対象の利用機関（拠点）
成果物 （受注者側で用意）	・設計・開発計画策定支援に係る資料など
仕様書に記載すべきポイント	設計・開発段階計画書の作成支援について、受注者が行うべき事項を記載する。 **【1.基本的に記載すべき要件】** ○設計・開発段階計画立案支援 **【2.案件の種類・特性によって追記すべき要件】**
仕様書記載上の例/説明	**基本的に記載すべき要件を記載している調達仕様書** ○設計・開発段階計画立案支援 受注者は、○○省が策定する設計・開発段階計画の作成を支援すること。 ・導入対象の利用機関 本調達にて導入対象とする利用機関は、「ネットワーク接続利用機関の帯域と利用期間」のとおりとする。 ・本調達に係る責任分界点 本調達に基づく責任範囲は、利用機関及びセンタに受注者が設置するネットワーク機器の間とする。
案件・情報システムの特性等による留意点	本役務の成果物として定められている設計・開発段階計画は、最適化ガイドラインにおける｢設計・開発段階計画｣に相当するものである。最適化ガイドラインでは、拡張時における当該成果物の作成を求めていないが、大規模な拡張を行うような場合には、関係者間の合意を得る必要性から当該成果物の作成を推奨する。 設計段階で要件定義を詳細化する作業を委託するケースもあると思われるが、その内容については6.2.2.要件定義段階における支援を参照のこと。
セキュリティに関する留意点	情報資産の重要度とリスクに応じた情報セキュリティ対策を、「政府機関の情報セキュリティ対策のための統一基準」に基づく各府省の情報セキュリティポリシーに準拠して、具体的に定義する。

2. 設計･開発

項目	内容
役務の概要	ネットワークの設計ならびに構築・施工・単体テストを行う。
想定されるインプット （発注者側で用意）	・ 設計・開発にあたって必要となるインプットとなるデータの参照、実施体制やプロジェクト管理方針、担当職員とのコミュニケーション、関連業者との責任分界点等に関する基本要件 ・ 導入対象の利用機関（拠点） ・ 既存の環境（ネットワーク構成図など） ・ 接続する上位組織のネットワーク情報（必要な場合） ・ 機器等を設置する場所における物理的な前提条件 ・ ネットワーク設計・開発に必要な技術要件 ・ サービスレベル項目定義（必要な場合）
成果物 （受注者側で用意）	・ 設計・開発実施計画書 ・ 基本設計書 ・物理設計 ・論理設計 ・信頼性設計 ・回線設計、外部接続設計 ・セキュリティ設計 ・ 詳細設計書 ・ 工事図面及び機器設置図 ・ 接続仕様書 ・ 設定書
仕様書に記載すべきポイント	ネットワークの設計・構築について、受注者が行うべき事項を記載する。 **【1.基本的に記載すべき要件】** ○設計・開発実施計画の内容 ○設計･開発業務実施者の満たすべき要件（スキル等）（必要な場合） ○設計業務の内容（基本設計、詳細設計、接続設計） －検討すべきと考えられる項目（詳細設定項目、LAN/WAN 接続設計項目、個別システムとの調整事項等）を含む ○開発業務の内容 －開発作業実施にあたっての留意点、実施要件を含む －テスト作業における実施要件を含む **【2.案件の種類・特性によって追記すべき要件】** ○LAN/WAN 接続設計や個別システム等との調整がある場合は、これらの作業に関する調達内容を明記する。 ○既存設備や機器の撤去・廃棄が必要な場合はその要件も記載する。

項目	内容
仕様書記載上の例/説明	**基本的に記載すべき要件を記載した例** ○設計・開発実施計画の内容 （1） 受注者は、○○省と調整しながら、設計・開発実施体制と役割、詳細な作業定義及びスケジュール、開発環境、開発方法、開発ツール等を含む設計・開発実施計画を定めること。 （2） 設計・開発実施計画に従って、設計・開発を行い、その結果を報告すること。 ○設計・構築業務実施者の満たすべき要件 本調達における設計・構築業務の管理を行う管理者は、以下の要件を満たすこと。《注：以下、当該役務相当の実績の要求、個人に要求する資格リスト又は資格保有者相当の能力の所有者であること、組織としての資格要件について記載する。法的に有資格者しか作業出来ない場合は、当該記載の有無に係わらず資格者の参画は必須である。具体的内容は省略》 ○設計業務の内容 (1) 基本設計 基本設計では、本調達の要件を最終確認後、具体的なネットワークサービスや機器を決定した上で、論理構成、物理構成等を記述すること。また、運用・保守に必要なセンタの設備についても設計すること。なお、設計に当たっては、継続利用する現行ネットワーク全体との関連において矛盾等が発生しないよう、ネットワーク全体として整合性が取れた内容とすること。 以下に、基本設計で実施する事項を示す。～詳細省略 ア. 設備設計(対象範囲の指定) イ. IP アドレス設計(ドメイン設計) ウ. ルーティング設計 エ. 物理構成設計(対象範囲の指定) オ. 論理構成設計(ネットワークトポロジー等) カ. 回線構成設計(バックボーン回線、中継回線、アクセス回線) キ. セキュリティポリシーに基づく設計(暗号化、FW、IDS/IPS、検疫) ク. 暗号化設計（暗号化仕様、暗号化方式、暗号化アルゴリズム) ケ. 帯域予約設計（帯域制御仕様、帯域制御方式) コ. 検疫システム設計（検疫仕様、検疫方式) (2) 詳細設計 詳細設計では、基本設計を基に当該ネットワークで運用される各

項目	内容
	機器等の主要な設定項目について、設定内容とともにその方針や理由を記述すること。 以下に、詳細設計で実施する事項を示す。なお、ここではネットワークと一体となって運用されるサーバ等に関する事項も記載している(6.7.機器調達付帯作業も併せて参照されたい)。　～詳細省略 ア. ネットワーク監視のパラメータ設計(ネットワーク監視パラメータ、サーバ監視パラメータ) イ. ネットワーク機器のパラメータ設計(ルータ、スイッチ等の設定値) ウ. サーバ機器の詳細設計(サーバの構成(冗長構成等)、ストレージ構成、ソフトウェア機能(OS、ミドルソフトウェア等)及びパラメータ設計 エ. セキュリティサービス(検疫等)のパラメータ設計 (3) 接続設計 接続設計では、関連部署・設備及び関連システム間の接続における物理構成や設定条件等を明確にすること。 以下に、接続設計で決定すべき事項を示す。～詳細省略 1). 情報センタ イ. 現行運用保守業者が運用する継続使用する現行ネットワークの提供サービスの受入方法 ウ. インターフェース仕様 エ. IP アドレス(ドメイン等) オ. ルーティング設計 カ. セキュリティポリシー設計(フィルタリング条件) キ. 暗号化設計（暗号化範囲）: 政府指針に基づき、適正な強度レベルの暗号を導入すること ク. 設置及び運用に係る設備仕様 2). ○○システム イ. 各種提供サービスの提供方法 ウ. インターフェース仕様 エ. IP アドレス(ドメイン等) オ. ルーティング設計(業務系ネットワーク及び情報系ネットワークへの通信経路の振分け) カ. 検疫システム設計（検疫適用の有無、検疫範囲、検疫対象機器の情報） キ. ファイアウォール/IDS/IPS 設計 ク. 本システムのネットワーク接続に係る設備仕様

項目	内容
	○開発業務の内容 　該当する設計内容に基づき、具体的な構築作業を行うこと。また、本内容を設計・構築に関する成果物にまとめること。 　以下に、開発業務で実施すべき事項を示す。～詳細省略 (1). 構築作業項目 　　イ．回線敷設作業 　　ウ．機器搬入・据付作業 　　エ．機器調整(単体テスト)作業 　　オ．機器設定・構築作業 (2) 回線敷設、機器搬入・据付作業 　ネットワークに接続する利用機関への回線工事、機器搬入、設置や動作確認の実施、移行完了後の利用者側での確認テスト等の問合せの支援を行う。 **案件の種類・特性によって追記すべき要件の記載例** ○LAN/WAN 接続設計や個別システム等との調整等を記載した例 (1) 既存の利用機関 　既存利用機関においては、（新規の回線導入ではなく）既存回線の増速を行うこととなるため、原則、導入作業は発生しない。 (2) 新たに接続する利用機関 　《注：下記項目等について、前提条件および設計、構築の条件を示すこと》 ・場所の確保、電源設備の確保 ・準備及び設置、電源の確保、配管に通す配線や機器の設置等の実施 ・利用機関管理者あるいは当該 LAN の管理業者との調整 ・前提事項 　各利用機関に機器等を設置する場合における物理的な前提条件を下記に示す。なお、下記の条件では対応できない利用機関等がある場合には、利用機関等の実態に応じた対応について担当職員及び利用機関と調整の上、実施すること。 　(1) 電源条件　～省略 　(2) 空調条件　～省略 　(3) 設置条件　～省略 ・ネットワーク要求仕様～詳細省略 　（構成を図示の上）ここに示すネットワーク構成に基づき、領域

項目	内容
	を WAN 環境、センタ接続環境に分け、環境毎に詳細な要求仕様を示す。 (1) WAN 環境 ・ 通信プロトコル及びルーティング方式 ・ 帯域予約 ・ セキュリティ要件 「○○省情報セキュリティポリシー」に従った対策を講ずること。 (2) センタ接続環境（新センタと既存センタの間を広域イーサ網などの WAN 回線を介し接続する環境） ・ 通信プロトコル及びルーティング方式 ・ セキュリティ要件 現行運用保守業者等と特に連携すべき事項があれば明記する（セキュリティ情報の共有方法、テスト方法、緊急時対策、など） ○機器の撤去、廃棄の要件を記載した例 (1). 撤去・搬出作業～詳細省略 作業内容の詳細を提示する。 ・ 不要となる機器の撤去作業 ・ 関連する配線の撤去作業 ・ 撤去の対象としないものの明示 ・ 撤去・搬出・廃棄のために必要なすべての経費（養生品、機材、車両等を含む）の負担の考え方 ・ 撤去・搬出日時、回数についての工程表の作成 ・ 必要な養生の実施 (2). データ消去作業 ア. データ消去作業に係る調整等は、担当職員から承認を得て、すべて受注者が行うこと。 イ. 不要機器の撤去・搬出後、第三者がデータ復元ソフトウェア等を利用してもデータが復元されないように完全にデータを消去すること。 ウ. データ消去作業に必要な場所や消去に必要な機器については、受注者の負担において用意すること。また、受注者は、不要機器の撤去、搬出からデータが消去されるまで、不要機器から情報が漏洩しないよう、厳重にセキュリティ管理をすること。なお、本省内で作業場所を提供する場合はこの限りではない。 エ. データ消去作業終了後、受注者は、データの消去完了を明記

項目	内容
	した証明書を担当職員に対して提出すること。 (3) 廃棄作業～詳細省略 作業内容･方法の詳細を提示する。 ア．廃棄に当たって関連法令を遵守のこと。再委託可能（ただし、当省に事前に通知し、承認を得ること）。 イ．廃棄作業完了後、廃棄完了証明書を提出する。 ウ．不要機器を破壊する場合以外について、データ消去作業を再委託する場合は、事前に担当職員の許可を得ること。 エ．当省は、作業内容を検査できるものとする。 オ．中古品としての再利用することも可。ただし、事前に承認を得ること。
案件・情報システムの特性等による留意点	・ 接続すべき既存システムがある場合は、所与の環境条件となるため、要件を適切に規定すること。 ・ 現行のネットワーク運用業者が存在する場合は、連携内容や条件について適切に規定すること。 ・ 記載例においてはデータ消去作業をオフサイトで実施する前提であるが、昨今の状況において、データの外部持ち出しはリスクが高いことから、オンサイトにおけるデータ消去を考慮する必要がある。 ・ 技術的要件や制約事項などの詳細要件を提案者が理解する必要がある場合はあわせて記載する。 －導入対象の利用機関（拠点）、既存の環境 －調達に係る責任分界点 －機器等を設置する場所における物理的な前提条件
セキュリティに関する留意点	セキュリティの重要性を踏まえ、下記のような要件・条件があれば明記する。 情報セキュリティ要件（対策） ➢ セキュリティ対策として、市場に認知されている対策全般を行うために、省のセキュリティポリシー、セキュリティガイドラインに従うこと。運用にあたっては、セキュリティレベルを維持すること。また、ネットワーク全体で講じなければならないセキュリティ対策については、現行運用・保守業者と協力、調整して行うこと。 機器の廃棄 ➢ 不要機器を破壊する場合以外は、データ消去作業について、撤去対象機器の撤去・搬出後、第三者がデータ復元ソフトウェア等を利用してもデータが復元されないように完全にデータを消去すること。

項目	内容
	セキュリティ設計 ➢ セキュリティポリシー設計(暗号化、FW、IDS/IPS、検疫)、暗号化設計（暗号化仕様、暗号化方式、暗号化アルゴリズム）等を実施するか、仕様と同時に提示された規定に従うこと。 セキュリティ検査 ➢ 導入するネットワーク機器の脆弱性について、第三者機関等において検証・公開されることがあり、問題がある場合は対応をすること。

3. 移行計画

項目	内容
役務の概要	新たに構築したネットワークへ切り替えるために必要な作業の計画を立案する。
想定されるインプット （発注者側で用意）	・ 移行条件（制約条件など） ・ 想定される移行作業フロー
成果物 （受注者側で用意）	⑴ 移行実施計画書 ・移行スケジュール ・移行時連絡方法 ・移行判定基準　等 ⑵ 移行手順書
仕様書に記載すべきポイント	新規に構築・拡張したネットワークと既存ネットワークを接続し、移行を実施又は支援する作業について、その要件ならびに計画立案に必要な項目等を記載する。 **【1.基本的に記載すべき要件】** ○移行方針･要件 ○移行計画策定業務の内容 **【2.案件の種類・特性によって追記すべき要件】**
仕様書上の記載例/説明	**基本的項目を記載した例** ○移行方針・要件～詳細省略 ア. 柔軟な計画 イ. 安定した稼動及び業務継続性の確保 カ. 利用者側でのアプリケーション接続テスト等での迅速なサポート。現行運用保守業者の支援が必要な場合には、発注者から依頼する イ. 個別システム管理責任者向け移行手順書及び利用機関責任者向け移行手順書の策定 ウ. 関係者との協議を行い、担当職員の承認と現行運用保守業者の確認を受ける範囲 ○移行計画策定業務の内容 移行を計画的に確実に実施するため、以下の事項について移行画を策定すること。 A. 移行に関する関係者及び受注者の移行実施体制と役割 B. 移行に係る詳細な作業及びスケジュール C. 移行環境 D. 移行方法

項目	内容
案件・情報システムの特性等による留意点	大規模の分離調達案件の場合、責任分解点が不明確になる恐れがあることから、予め役割分担表を作成するなどして明確化しておく必要がある。 ネットワークが複数のセンタ設備を持つ大規模なものである場合、センタ設備ごとに単体・結合テストを済ませたのち、移行作業と同時に終端装置の設置や接続工事を行う場合もあり、その際は、前節の設計・構築における「回線敷設、機器搬入・据付作業」を本節および次節の移行役務の一部として記載したほうが実態に近くなる可能性もある。
セキュリティに関する留意点	－

4. テストと移行判定支援

項目	内容
役務の概要	新ネットワークが設計どおりの動作を行うことを確認するため、システムを利用者に供する前に各種のテストを実施する。
想定されるインプット （発注者側で用意）	**・テストの実施要件** **・(発注者が実施する)受入テストの概要** **・移行判定基準(あるいは、受入テスト合格基準)**
成果物 （受注者側で用意）	・テスト実施要領 ・テスト計画書 ・テスト結果報告書
仕様書に記載すべきポイント	テストの計画立案から実施までの役務提供を求める。テスト実施内容については、主に実施すべきテスト項目（案）を定める。 **【1.基本的に記載すべき要件】** ○テスト計画の作成 ○テストの実施（実施内容の記載） ○進捗・課題管理の実施 ○結果報告 ○受入テスト支援 **【2.案件の種類・特性によって追記すべき要件】** ○新システム切替え判定支援と本稼働可否の協議
仕様書上の記載例/説明	**基本的に記載すべき要件を記載した例** ○テスト計画の作成 テスト体制と役割、詳細な作業及びスケジュール、テスト環境、テストツール、合否判定基準等を記したテスト実施計画を作成する。 ○テストの実施（実施内容の記載） 次の内容について新システムのテストを実施し、設計どおりの稼働が行われていることを確認すること。～テストの内容詳細については省略 ・拠点間テスト ・業務システムとの接続テスト ・情報セキュリティ確認テスト ・総合テスト ・運用テスト(受入テスト、ユーザテスト)支援 ○進捗・課題管理の実施 受注者は、テスト作業開始前にテスト計画書に基づくテストの進捗状況、作業上の課題等についての管理・報告ルールを提示し、○○省の承認を得ること。受注者は、その後にルールに沿った管理・報告を行うこと。 ○結果報告

項目	内容
	受注者は、テストの結果を「テスト結果報告書」として取りまとめ、○○省の承認を得ること。 ○受入テスト支援 ○○省は、受注者等が総合テスト等を終了した後に、新システムが要件に適合しているかを検証するため、受入テストを行う。 受注者は、○○省が策定する受入テスト実施計画、受入テスト仕様書の作成及び受入テストの実施を支援すること。 ・その他 （1） テストに当たって、現行システムのデータ等を利用したい場合には○○省に申し出ること。なお、○○省は正当な理由があると判断した場合に限りデータ等を提供する。受注者は、提供されたデータ等の取扱いに十分留意すること。 （2） テストに当たって、必要な機器及び通信回線等については、受注者において準備すること。 **移行判定支援を役務要件としている例** ○移行判定に係る支援 移行判定とは、新ネットワークへの切替の実施の可否について、新ネットワーク側と関連する個別システム側で最終的な判断を行うことである。そのため、受注者は、現行運用保守業者と協力し、担当職員の指示に基づき以下の作業を実施すること。 ア. 作業状況、懸案事項、○○システムに対する確認事項等を記載した移行判定基準の作成に際して支援を行う。 イ. 移行判定基準に沿って、担当職員、現行運用保守業者、受注者、PMO 及び個別システム管理責任者で構成される移行判定会議を開催し「移行判定基準」の確定及び○○システムの新ネットワークへの切替の最終判断について合意する。
案件・情報システムの特性等による留意点	3. 設計・開発を参照
セキュリティに関する留意点	情報セキュリティに関するテストの実施を確実に行うこと。 導入するネットワーク機器の脆弱性について、第三者機関等において検証・公開されることがあり、問題がある場合は対応をすること。

5．移行

項目	内容
役務の概要	移行を実施する。
想定されるインプット（発注者側で用意）	・発注者と受注者の役割分担
成果物（受注者側で用意）	・移行結果報告書
仕様書に記載すべきポイント	移行実施にあたっての方針、要件ならびに実施事項を記載する。 **【1.基本的に記載すべき要件】** 〇移行実施の方針 〇移行作業内容 **【2.案件の種類・特性によって追記すべき要件】**
仕様書上の記載例/説明	**センタと導入機関など拠点間ネットワーク接続を伴う移行作業の仕様書例** 〇移行実施方針 ア．移行作業において、障害発生等により作業が中断した場合、影響する関係者に第一報の連絡を行うこと。なお手順については、計画で策定した報告手順に従って行うこと。 イ．ネットワーク接続により既存システムで問題が発生した場合には、協力して原因調査にあたること。利用機関等に対応要員を派遣する必要がある場合には、その手配と利用機関との調整を行うこと。 エ．移行・導入の際に先に稼働している個別システム等に影響があると想定される場合には、事前に担当職員及び個別システム管理責任者に連絡をすること。 ウ．移行・導入工事作業完了後、利用機関責任者に作業完了連絡を行い、環境の引渡しを行うこと。また、担当職員及び現行運用保守業者に対しても報告を行うこと。 エ．想定する主たる業務フローは、参考資料に示すとおりである。なお、効率化等の目的で本業務フローを変更する必要がある場合には、担当職員の承認を得ること。 〇移行作業内容
案件・情報システムの特性等による留意点	・ 既存回線の拡張の場合などは、既存システムとの併用が重要となるので、現行の運用・保守業者への報告等の作業を含めることを検討する。 ・ 調達されるネットワークの規模や既存システムの有無など、実際の条件によって記載内容を調整する。
セキュリティに関する留意点	－

6. 運用･保守計画

項目	内容
役務の概要	運用・保守のための体制づくりと運用設計、ドキュメント整理を行う(ネットワーク関連の保守は、一般に特別な知見を必要とするものでなく、むしろ運用と一体化したほうが効率的であると考えられる)。
想定されるインプット （発注者側で用意）	・導入・運用等の期間、借入期間、支払期間 ・構成管理項目 ・ 構成管理書様式 ・ネットワークの運用に係るセキュリティポリシー ・運用・保守情報セキュリティマニュアル
成果物 （受注者側で用意）	・運用･保守要領 ・運用設計書 ・運用マニュアル ・利用機関責任者及び個別システム管理責任者用マニュアル ・構成管理システム又はマニュアル ・ サービスレベル合意書（SLA） ・ サービスレベル管理計画書
仕様書に記すべきポイント	運用・保守開始準備に関する項目、役務要件を記載する。 **【1.基本的に記載すべき要件】** ○運用・保守業務実施者が満たすべき要件 ○運用・保守の基本要件 ○運用・保守設計の実施 －運用設計 －構成管理書（ホスト名、IP アドレス等）作成と維持責任者用マニュアルの作成 －サービスレベル管理計画立案 ○運用・保守業務における体制と役割分担 **【2.案件の種類・特性によって追記すべき要件】** ○現行運用事業者からの引き継ぎ

項目	内容
仕様書上の記載例	**基本的な項目を記述した例** ○運用・保守業務実施者が満たすべき要件 　本調達における運用・保守業務の管理を行う管理者は、以下の要件を満たすこと。 (5). セキュリティ管理者 　本調達におけるセキュリティ管理を行う責任者は、以下の要件を満たすこと。 ア.情報セキュリティを保つための施策を計画・実施し、その結果に関する評価を行った実績を有すること。 ○運用・保守の基本要件 (1) 安定的、効率的なシステム運用・保守基盤の確立 ア. ネットワーク全体の運用・保守については、現行運用保守業者が実施しているため、受注者は担当職員又は調達担当課室の指示に従う他、運用・保守総括の立場としての現行運用保守業者の助言に従うこと。 以下、詳細は省略 (2) 利用者への高品質なサポート提供 ア. 本調達部分の利用者へのサポートを行う窓口を、現行運用保守業者が実施している窓口に一元化し、利用者の利便性を図るので、それを踏まえること。 以下、詳細は省略 (3) サービス品質のモニタリングと継続的な改善 ア. 現行運用保守業者と調整の上、サービスレベル項目に関する数値のモニタリングを行い、結果を評価し、担当職員への報告を行うこと。 以下、詳細は省略 (4)運用・保守業務におけるセキュリティ管理の実施 ア.〇〇省の情報セキュリティポリシーを遵守すること。また、遵守されていることを確認できる仕組みとすること。 イ. セキュリティ運用マニュアルに基づいて、訓練・運用を実施すること。 ウ. セキュリティイベントが発生した場合には、現行運用保守業者とともに、担当職員への報告と対策を施すことが可能な仕組みとすること。

項目	内容
	○運用・保守設計の実施 （運用、保守設計を行い、）以下の文書を作成すること。 (1). 運用・保守要領 最適化ガイドラインにおける「運用・保守要領」に相当するもの (2). 運用基本設計書 ネットワークの運用体制及び各種手順等を定めた成果物 (3). 運用マニュアル 機器利用及び障害発生時等におけるネットワークの運用に係る担当者の作業手順等を定めた成果物 (5). 利用機関責任者及び個別システム管理責任者用マニュアル 利用機関責任者及び個別システム管理責任者向けに、ネットワークを利用するために必要な各種設定、操作方法及び申請方法等を示した成果物 (6). 構成管理書 ネットワークを構成する各ネットワーク機器及び設定に関する成果物 (9). SLA 及びサービスレベル 管理計画書 最適化ガイドラインにおける「サービスレベル合意書(SLA)」に相当するもの、およびサービスレベル管理計画書 ○運用・保守業務における体制と役割分担 想定する運用・保守業務の体制と主な役割分担を示す **案件の種類・特性によって追記すべき要件** ○現行運用事業者からの引き継ぎ
案件・情報システムの特性等による留意点	重要システムについては SLA を定めることを強く推奨する。
セキュリティに関する留意点	—

7. 運用・保守業務

項目	内容
役務の概要	運用・保守開始準備の結果を受けて、運用を行う。
想定されるインプット （発注者側で用意）	(運用・保守開始準備で作成された、運用・保守に係るドキュメント)

項目	内容
成果物 （受注者側で用意）	ネットワーク運用報告書 ・ 運用状況 　・ インシデント状況 　・ 稼動実績 　・ 消耗品の状況 ・ 保守・点検状況 ・ SLA 遵守状況等
仕様書に記載すべきポイント	ネットワーク運用に関する役務作業およびその実施要件等を記載する。 **【1.基本的に記載すべき要件】** 〇構成管理・変更管理業務 〇保守業務 〇監視業務 〇障害対応業務 **【2.案件の種類・特性によって追記すべき要件】** 〇関連するネットワークシステムの運用・保守業者が既にいる場合の要件･･･以下の例示では、これを前提としている
仕様書上の記載例/説明	**運用・保守業務の基本的な項目＋既存運用・保守業者がいる場合の記載例** 〇構成管理・変更管理業務 構成管理・変更管理業務は、ネットワークに接続された利用機関の接続設定の変更や移設を実施し、構成情報を最新に維持管理する一連の業務である。 現行運用保守業者に実施を委託しなければならない業務については、その内容を詳細に発注者に申請すること。 (1). 対象 本調達において「構成管理・変更管理業務」の対象となるのは、新規にネットワークと接続した利用機関、新センタ及び新規に受注者が導入した機器(回線の増速に伴い更改した機器を含む)である。単に回線増速を行った利用機関に関しては、引き続き現行運用保守業者が実施することとする。 (2). 業務内容～詳細省略 ア. 構成管理・変更管理業務手順の見直し イ. ネットワーク接続内容の変更申請（省内事務手続き処理） ウ.変更作業日程及び作業内容、依頼事項などの調整、実施計画作成 エ. 変更が必要となる場合は、回線種別の変更や機器変更等の準備

項目	内容
	オ．必要な場合には、申請者と調整を行い現地調査 カ．ネットワークの疎通確認テスト キ．ネットワーク環境の引渡し ク．環境の引渡し後問題が生じた場合には、協力して原因調査にあたること ケ．構成管理情報を更新し最新の構成を維持管理するまで、7 日以内とする 〇保守業務 保守業務は、ネットワークを構成する機器を維持するために、必要に応じ保守点検作業を行う一連の業務である。 (1)．対象 本調達において「保守業務」の対象となるのは、新規にネットワークと接続した利用機関、センタ及び新規に受注者が導入した機器(回線の増速に伴い更改した機器を含む)である。単に回線増速を行った利用機関は、引き続き現行運用保守業者が実施することとする。 (2)．業務内容～詳細省略 ア．サービス実施計画について見直し イ．作業に関する現行運用保守業者、個別システム管理責任者、利用機関責任者と、作業日程、作業内容、依頼事項等必要となる調整 ウ．ネットワークとしての疎通確認テスト エ.ネットワーク環境の引渡し オ．保守点検作業の記録・管理 カ．保守のための稼動停止の連絡 〇監視業務 監視業務は、セキュリティの観点から、本調達部分も含めネットワーク全体で行う必要があるので、本調達により構築されるセンタ及び回線を増速、あるいは新規接続する利用機関についても、現行運用保守業者に一括して監視業務を実施させる。ただし、受注者が本調達に基づき提供するバックボーン回線の監視業務は、受注者が行うこと。 ア．本調達に基づき、回線を提供する業者から、回線に関する障害情報を迅速に受け、対応する連絡体制を確立すること。 イ．設定、閾値等の調整を行う必要がある場合には、担当職員及び関係者の承認を得て実施すること。また、利用者からの設定の変更要望についても検討を行い、設定の調整を行うこと。

項目	内容
	○障害対応業務 　障害対応業務は、ネットワークを構成する回線、機器等に障害が発生した場合の復旧に関する一連の業務である。以下に示す業務内容を実施すること。 (1). 対象 本調達において「障害対応業務」の対象となるものは、新規にネットワークと接続した利用機関及びセンタ、並びに新規に受注者が導入した機器(回線の増速に伴い更改した機器を含む)である。 単に回線増速を行った利用機関は、引き続き現行運用保守業者が実施することとする。 (2). 業務内容～詳細省略 　ア. 現行運用保守業者業務への協力 　イ. 受注者自らが実施する業務
案件・情報システムの特性等による留意点	構成管理要件については、既存の資産管理を含めて発注者が提示する。 　ヘルプデスク業務について、現行運用保守業者に一括して実施させる場合は、現行運用保守業者がヘルプデスク業務を円滑に実施できるよう受注者が協力を行うことを要請する。
セキュリティに関する留意点	インシデント対応 ➢ ネットワークに関する障害情報及びセキュリティインシデントを迅速に受けられる連絡体制を確立すること。 セキュリティ診断と報告 ➢ 回線のトラフィック状態を常時監視すること。異常なトラフィック等があった場合には、早急に原因調査を行い、現行運用保守業者を経由して担当職員に報告をすること。 セキュリティ検査 ➢ 導入するネットワーク機器の脆弱性について、改善の必要性が指摘された場合には、迅速に対応すること。

6.9.2.2.納入成果物と提出のタイミング

納入成果物とタイミングをまとめると、下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即した記載をする必要がある。

役務	納入成果物	納入期限
1.設計・開発計画	設計・開発計画策定支援に係る資料など	設計・開発作業開始前までに
2.設計・開発	設計・開発実施計画書	設計の文書策定時
	基本設計書	
	詳細設計書	
	工事図面及び機器設置図	
	接続仕様書	
	設定書	
3.移行計画	移行実施計画書	移行計画の文書策定時
	移行手順書	
4.テストと移行判定支援	テスト実施要領	テスト計画の文書策定時
	テスト計画書	
	テスト結果報告書	接続テスト完了後
5.移行	移行結果報告書	移行完了後
6.運用･保守計画	運用･保守要領	運用･保守計画の文書策定時
	運用設計書	
	運用マニュアル	
	利用機関責任者及び個別システム管理責任者用マニュアル	
	構成管理システム又はマニュアル	
	SLA、サービスレベル管理計画書	
7.運用･保守業務	ネットワーク運用報告書	運用開始後、月次

6.9.2.3.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると、下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即した記載をする必要がある。

役務	インプット	インプットを提示する タイミング
1. 設計･開発計画	開発スケジュール	入札公示時
	府省の意見	
2. 設計･開発	基本要件	入札公示時
	導入対象の利用機関（拠点）	
	既存の環境（ネットワーク構成図など）	仕様書にて概要、契約後に詳細
	機器等を設置する場合における物理的な前提条件	入札公示時。内容により契約後
	ネットワーク設計･開発に必要な技術要件	入札公示時
	サービスレベル項目定義（必要に応じて）	
3. 移行計画	移行条件	入札公示時
	想定される移行作業フロー	
4. テストと移行判定支援	テストの実施要件	入札公示時
	受入テストの概要	
	移行判定基準	
5. 移行	発注者と受注者の役割分担	入札公示時
6. 運用･保守計画	導入･運用等の期間、借入期間、支払期間	入札公示時
	構成管理項目	
	構成管理書様式	契約後
7. 運用･保守業務	（運用･保守開始準備で作成された、運用･保守に係るドキュメント）	入札公示時

サービスレベル項目定義の例:ここに挙げた項目、設定値などはあくまで例であり、調達に当たっては十分な検討と合意に基づくものとすることが必要である。

１）サービスレベル項目（抜粋）

ネットワーク機器は障害発生時の影響範囲が広く、重要度も高いことから、サービスレベル項目として設定する。

対象は以下のとおりで、評価単位は(別途定める)サービス毎とする。

A. インターネット接続を構成するネットワーク機器

B. 内部接続を構成するネットワーク機器

サービスレベル項目	説明	設定値
稼働率	稼働予定時間に対して実際に稼働した時間（稼働時間）の割合である。	99.9%以上
平均故障復旧時間（MTTR）	サービス稼働時間中において、機器に故障が発生した時刻から故障が復旧した時刻までに要した時間の1 ヶ月間における平均値である	1時間以内
平均故障間隔（MTBF）	機器に故障が発生してから、次に故障が発生するまでの平均時間である。	2920 時間（4 ヶ月）以上

障害・問合せへの初動に関するサービスレベル項目

サービスレベル項目	説明	設定値
障害・問合せの発生から初期レスポンスまでのリードタイム	ヘルプデスク稼働時間中に、障害・問合せが発生した時刻から、担当職員及び連絡してきた利用者に対して、その内容についての把握状況、初動等に関する状況を報告するまでの時間	15 分以内

（２）SLA 遵守に関する規定

SLM（Service Level Management）の目的は、業務に必要とされるサービスレベルを担当職員と受注者が協力しながら、達成、維持、及び改善することにある。したがって、SLA で規定された目標値を達成できなかった場合は、受注者は担当職員と連携し、より一層の改善努力を行うことにより、サービスレベルを達成させることが重要である。

利用者が国民である情報システム、社会的なインフラ及びシステム全体に影響を与えるインフラとして提供するサービスにおいては、その重要性を考慮し、サービスレベル目標値に対して未達成の場合、金銭的なペナルティを課す(SLM の設定、SLM の実施を踏まえてのペナルティ、インセンティブとする)。

（３）ペナルティ及びインセンティブの考え方

ア. 落札金額の 90%を受注者の基本報酬、残り 10%の金額を SLA 遵守状況に応じた成功報酬として扱い、月次の SLA 達成状況の報告をベースに評価し、「達成度合い」に応じた額を基本報酬に上乗せした形で、月単位の報酬として支払うこと

とする。

イ. サービスレベル項目について、対象となる個別サービス･機器単位で、サービスレベル設定値に対する達成状況を月次で評価する。また、サービスレベル設定値の未達成項目の数より、当該月の「達成度合い」を 4 段階にて評価する。

（4）SLA の評価期間

SLA の遵守については、稼働開始日からとする。ただし、支払額の変動は、サービス開始後 3 ヶ月目からの開始とする。

（5）サービスレベル目標値未達成が継続している場合の措置

ア. 損害賠償請求

SLA の遵守率が著しく低く、改善の見込がない原因が受注者にある場合、別途、契約金額を上限とした損害賠償を課す場合がある。SLA の遵守率が著しく低いと判断する達成度合いの継続期間及び回数は、以下のとおりとする。

A. 「達成度合い D」の状況が、「3 ヶ月以上連続」、「年間 4 回以上」、及び「稼働期間の通算で 12 回以上」のいずれか

B. 「達成度合い C」の状況が、「5 ヶ月以上連続」、「年間 6 回以上」、及び「稼働期間の通算で 18 回以上」のいずれか

C. 障害発生等のために、業務遂行不可能な状況により、落札額の 10%とした成功報酬相当額を上回る規模の損害が発生した場合

イ. 入札資格の剥奪

特に、上記「ア」の状況にいたる場合は、当省の要求する品質のサービスレベルを提供する能力がないものと判断し、受注者としての資格の一定期間の剥奪、契約の解除、更には次回契約更改時の入札資格停止等のペナルティを課すこともある。

6.9.2.4.役割分担

既存のネットワークと併存する形で調達する場合、運用･保守における利用者とネットワーク運用者の役割分担の記載例

体制		主な役割	備考
利用者	個別システム管理者	・ 各システム側の責任者として運営主体との調整窓口となる ・ 作業時の立会い、障害時の切り分け、原因調査の支援等を行う	個別システム毎に配置
	利用機関責任者	・ 利用機関の責任者として運営主体との調整窓口となる ・ 利用機関側の環境整備、作業時の立会い、障害時の支援等を行う	利用機関毎に配置
統合ネットワーク運営主体	受注者	・ 運用･保守計画（実施手順マニュアル整備等）の作成の協力を行う ・ 運用･保守計画に従い、構成管理･変更管理、保守、障害対応、定期報告の業務を実施する ・ サービス品質のモニタリング項目に対して、モニタリング、評価、分析、改善を行う ・ 実施状況を運営主体（担当職員）に対して報告を行うための、現行運用保守事業者への情報提供を行う	受注範囲に関する部分
	現行運用保守業者	・ 運用･保守業務の統括･管理を行う ・ 蘊奥･保守計画（実施手順、マニュアル整備、スケジュール等）の策定を行う ・ 運用･保守計画に従い、公正管理･変更管理、保守、監視、障害対応、ヘルプデスク、定期報告の業務を実施する ・ サービス品質のモニタリング項目に対して、モニタリング、評価、分析、改善を行う ・ 実施状況を運営主体（担当職員）に対して報告する	
	担当職員 (工程管理支援業者を含む)	･運営主体として運用･保守における意思決定及び最終承認を行う	2 名程度 (工程管理支援業者は別)

既存のネットワークと併存する形で調達する場合、運用･保守における既存ネットワーク運用事業者と受注者の役割分担の記載例

No.	項目	説明	現行運用保守業者の役務	受注者の役務 (受注範囲に関する部分)
1	運用統括業務	運用･保守業務における業務全般の統括･管理業務	○	×
2	構成管理･変更管理業務	ネットワークに係る各種申請への対応及び構成変更管理等を行う業務	○	○
3	保守業務	ネットワークを構成する機器を維持するため、筆意うに応じて実施する保守業務	○	○
4	監視業務	ネットワークを構成する回線、機器等の稼動状況を把握するための監視業務	○	△ (バックボーン回線の監視のみ)
5	ヘルプデスク業務	ネットワークに係る問合せ対応及び情報提供を行う業務	○	×
6	障害対応業務	ネットワークを構成する回線、機器等に障害が発生した場合の復旧作業業務	○	○
7	運用･保守に係る実施状況の報告業務	運用･保守業務における全般的な状況、SLA の達成状況、品質監査について、ネットワーク運営主体へ定期的に報告する業務	○	○
8	セキュリティ管理業務	ネットワークのセキュリティ維持に係る業務	○	△ (セキュリティインシデント対応)

6.9.3.通信サービスの調達に係る役務

6.9.3.1.仕様書に記載すべき役務内容

6.9.3.1.1.代表的な役務の内容

役務	役務の概要	SLCP の アクティビティ	調達基本指針に対応する仕様書の章･節 （及びそのタイトル）
1.導入準備	スケジュールの作成 実施手順に関する府省側との調整 事前調査などの準備作業	3.2.1 （環境整備）プロセス開始の準備	2章（4）、(5) 4章、5章、6章、 10章、11章
2.導入	サービス提供に必要な工事等	2.2 環境の構築 2.3.1 品質保証プロセス開始の準備	
3.運用管理･保守	サービス提供を継続的に行うための運用･保守	1.7.7 システム運用の評価 1.8.2 問題把握及び修正分析 1.8.3 修正の実施	5章(5)、10章、11章、12章
4.報告	ネットワークサービス運用に伴う定期報告	1.7.4.1 システムの運用、 1.7.4.2 運用監視及び運用データの収集、問題の識別、記録及び解決、運用環境の改善 1.7.4.3 問題の識別及び改善 1.7.4.4 運用環境の改善 1.7.7 システム運用の評価	

6.9.3.1.2.各役務内容に関する説明及び仕様書上の記載例

1．導入準備

項目	内容
役務の概要	スケジュールの作成、実施手順に関する府省側との調整、事前調査などの準備作業を行う。
想定されるインプット （発注者側で用意）	・スケジュールの概要 ・機能仕様 ・ 導入拠点一覧 ・ 機器（ODU、分電盤等）設置予定場所、電源/通信ケーブル管路や配線予定場所等を示した平面図
成果物 （受注者側で用意）	・詳細な導入スケジュール ・建物内現地調査報告書
仕様書に記載すべきポイント	通信サービス導入の準備作業について、受注者が行うべき事項を記載する。 **【1.基本的に記載すべき要件】** 〇詳細な導入スケジュールの確定および府省側との調整の実施 －導入にあたっての基本要件、留意事項も記載 〇事前調査の実施 〇提供期間、提供場所 **【2.案件の種類・特性によって追記すべき要件】** 〇調達するネットワークサービスの機能仕様等を記載
仕様書記載上の例/説明	**サービスを調達する場合の調達仕様書例** 〇詳細な導入スケジュールの確定および府省側との調整の実施 ・ スケジュールの概要は、「導入スケジュール案」のとおりとし、落札後 10 日以内に担当職員と協議の上、詳細な導入スケジュールを決定するものとする。ただし、スケジュール決定後、諸般の事情から当省と受注者の協議により日程を変更することもある。 ・ 受注者は、必要に応じて〇〇システム受注者と調整すること。 〇事前調査の実施 ・ 受注者は、当省の各拠点の建物内現地調査（建物内のケーブルの敷設方法及び経路の確認、提出すべき書類等の有無、専門の建物管理業者の有無、配管工事等の建物内工事の必要性の有無の確認等をいう。）を行い、担当職員に調査内容の報告を調査拠点の立面図・平面図を付与し書面等にて行うこと。また、当省より提出すべき書類があれば、この時点で担当職員に申し出ること。 ・ 現地調査において配管にかかわる建物内工事等、敷設に必要な

項目	内容
	付帯工事が発生した場合には、別途、見積を提出すること。 **調達するネットワークサービスの機能仕様の記載例** ○機能仕様 (1) インターネット接続サービス～詳細は省略 インターネットサービスプロバイダ（以下「ISP」という。）として、以下の仕様を満たすインターネット接続を提供すること。 ① 帯域 ② 当省に引き渡される際のインターフェース ③ ISP としての条件 ⑤ドメインに関する申請代行 ⑧ IP アドレスの割当てについて ⑪ セカンダリ DNS サービス等 ⑫ 受注者の相互接続点と当省間のアクセス回線他の条件 ⑮ インターネット接続サービスの接続帯域及び回線種別の変更等を行う場合の通信料等の料金の条件 (2) WAN 回線(広域イーサネットサービス) ○○省本省と地方支分部局等のすべての拠点に広域イーサネットサービスによるネットワークを提供し、提供に当たっては、以下の要件をすべて満たすこと。なお、拠点の所在地及び接続帯域については、「各拠点の所在地と帯域一覧」を参照すること。 要件詳細については省略 (3) ○○システムとの接続 詳細は省略 ○提供期間、提供場所 (1) 提供期間 ● 平成○○年○○ 月○○ 日～平成○○ 年○○ 月○○ 日 (2)提供場所 ● インターネット接続サービス ○○省コンピュータセンタ内 ● 広域イーサネットサービス「各拠点の所在地と帯域一覧」参照
案件・情報システムの特性等による留意点	既存の LAN、WAN がある場合、また他に関連システムの調達が同時期になされている場合は、導入作業実施にあたって特に調整を要する事項について記載すること。
セキュリティに関する留意点	ー

2. 導入

項目	内容
役務の概要	サービス提供に必要な工事等を行う。
想定されるインプット （発注者側で用意）	—
成果物 （受注者側で用意）	・ 導入結果報告書 ・ 工事図面（機器（ODU、分電盤等）の設置場所、ケーブル敷設箇所を示した図面）
仕様書に記載すべきポイント	通信サービスの導入に関して、受注者が行うべき事項を記載する。 **【1.基本的に記載すべき要件】** ○導入作業内容と留意事項 ○調整を要する事項等 **【2.案件の種類・特性によって追記すべき要件】**
仕様書記載上の例/説明	**インターネット接続サービスならびに広域イーサネットサービスを調達する場合の調達仕様書例** ○導入作業内容と留意事項 ・ 本作業に起因して受注者の責に帰すべき○○システム、インターネット接続サービス、○○省 WAN の障害が発生した場合には、代替機能を受注者の負担で提供すること。 ・ 受注者は、通信回線開通日までに運用体制表及び障害発生時の対応マニュアルを作成し、担当職員の了承を得ること。また、障害からの早期復旧のため、担当職員が行える軽微な作業があれば、当該作業内容をマニュアルに記載すること。 ・ 担当職員が受注者に対し、常時契約履行に関する確認を行える体制とすること。 ・ インターネット接続サービス並びに広域イーサネットサービスの提供が、開通予定時期に間に合わず、それが受注者の責任に帰する場合、受注者は、現在、当省が契約している WAN 回線並びにインターネット接続をそのまま維持するか、又は代替案を提案し、担当職員の了承を得た上で措置すること。この場合に必要となる一切の費用は受注者の負担とする。 ○調整を要する事項等 ・ 当省の拠点の工事に当たり、受注者は、法令等に定められた手続が必要な場合、官公庁等に対し手続を行うこと。また、手続完了後に担当職員に報告すること。 ・ 工事に際し、造営物及び道路の損傷、土地踏み荒らし等、第三者に与えた損害に対する費用等は、すべて受注者の負担とす

項目	内容
	る。 ・　当省の拠点へ工事に入る場合、受注者は、その 2 週間前までに詳細な施工及び作業の内容、範囲、作業員名、スケジュール及び使用車両を担当職員に書面等で提出し了承を得ること。
案件・情報システムの特性等による留意点	既存の LAN、WAN がある場合、また他に関連システムの調達が同時期になされている場合は、導入作業実施にあたって特に調整を要する事項について記載すること。
セキュリティに関する留意点	－

3. 運用管理･保守

項目	内容
役務の概要	サービス提供を継続的に行うための運用管理・保守を行う。
想定されるインプット （発注者側で用意）	サービスレベル項目（SLA 締結を要求する場合） 運用要件
成果物 （受注者側で用意）	－
仕様書に記載すべきポイント	通信サービスの運用管理・保守に関して、受注者が行うべき事項を記載する。 **【1.基本的に記載すべき要件】** ○運用管理・保守作業内容 ○運用作業における留意事項 **【2.案件の種類・特性によって追記すべき要件】**
仕様書記載上の例/説明	**サービスを調達する場合の調達仕様書例** ○運用管理・保守作業内容 ・ 受注者は、24 時間×7 日間/週体制でネットワークの監視及び障害受付ができる体制があること。また、障害の早期発見及び迅速な復旧を行う観点から、インターネット接続サービス並びに広域イーサネットサービスの監視及び障害受付の窓口は一本化すること。 ・ 受注者は、障害を検知後、停止時間が原則として 5 分以上継続した場合、直ちに担当職員に通知すること。また、受注者は、障害復旧するまで、原則として 30 分ごとに状況報告を担当職員に行うこと。ただし、担当職員の指示があればこの限りではない。 ・ 受注者は、障害発生に備え、24 時間×7 日間/週の故障修理・復旧対応を行える体制であること。障害を検知した場合、SLA を遵守すべく速やかな障害復旧に努めること。 ・ 受注者は、障害が発生した場合、適切な再発防止策を受注者の負担で実施すること。 ○運用作業における留意事項 ・ 計画的な工事及び定期的な保守等を行う場合、受注者は、できるだけネットワークを停止させずに実施すること。なお、やむを得ずネットワークを停止し、計画的な工事及び定期的な保守等を行う場合、受注者は、少なくともその 2 週間前までに担当職員に連絡し了承を得ること。 ・ 受注者は、運用を続けると明らかに障害に至ることが分かって

項目	内容
	いてネットワークを緊急停止する場合、担当職員と協議の上、対応を決めること。
案件・情報システムの特性等による留意点	システムの状況によっては、特に、監視及び障害受付の窓口一本化を要求することを検討すること。
セキュリティに関する留意点	－

4. 報告

項目	内容
役務の概要	ネットワークサービス運用に伴う定期報告を行う。
想定されるインプット（発注者側で用意）	－
成果物（受注者側で用意）	・運用報告書 ・ＳＬＡの達成状況に関する報告書
仕様書に記載すべきポイント	通信サービスの運用報告について、受注者が行うべき事項を記載する。 **【1.基本的に記載すべき要件】** 〇報告内容 **【2.案件の種類・特性によって追記すべき要件】**
仕様書記載上の例/説明	**サービスを調達する場合の調達仕様書例** 〇報告内容 ・ 受注者は、インターネット接続サービスについては、月初めに前月分のトラフィック情報を担当職員のみが確認できるようWeb 形式又はメール添付可能な CSV 形式にて提供すること。広域イーサネットサービスについては、日、週及び月単位で回線ごとのグラフ化したトラフィック情報を、Web 上で担当職員のみが確認できる仕組みにて提供すること。 ・ 受注者は、原則として毎月 1 回、当省のインターネット接続サービス並びに広域イーサネットサービスを熟知した運用担当者が参加し、サービスレベル各項目の前月分の達成状況及び障害対応についての報告会を担当職員に行うこと。SLA 未達成の場合には、その原因を分析して担当職員に報告し、必要に応じてサービス改善等の措置について協議すること。
案件・情報システムの特性等による留意点	関連システムとの接続にかかる信頼性についても報告することが必要であれば、その旨明記すること。
セキュリティに関する留意点	－

6.9.3.2.作成すべき納入成果物と提出のタイミング

納入成果物とタイミングをまとめると下記の通りとなる。各成果物の正式名称、納入期限に関しては実態に即した記載をする必要がある。

役務	納入成果物	納入期限
1. 導入準備	詳細な導入スケジュール	落札後 10 日以内
	建物内現地調査報告書	導入準備中の現地調査実施後
2. 導入	導入結果報告書	導入作業完了時
3. 運用管理･保守	—	—
4. 報告	運用報告書	運用開始後、月次又は適宜
	ＳＬＡの達成状況に関する報告書	

6.9.3.3.想定されるインプット

受注者（もしくは提案者）に対して事前に提示すべきインプットとタイミングを記載すると、下記の通りとなる。各インプットの正式名称、納入期限に関しては実態に即した記載をする必要がある。

役務	インプット	インプットを提示する タイミング
1. 導入準備	スケジュールの概要	入札公示時に調達仕様書･付属資料に記載する
	機能仕様	入札公示時に調達仕様書･付属資料に記載する
	導入拠点一覧	入札公示時に調達仕様書･付属資料に記載する
2. 導入	—	—
3. 運用管理･保守	サービスレベル項目	入札公示時に調達仕様書･付属資料に記載する
4. 報告	—	—

サービスレベル項目の記載例:

5. SLA

(1) 当省からIX(Internet eXchange) までのネットワーク及び○○省 WAN を構成するネットワークは、高い信頼性を有し、バックボーンの稼働率及び提供するすべてのアクセス回線の毎月の稼働率がそれぞれ 99.9%以上であること。

(2) 稼働率の定義を以下に示す。

- インターネット接続サービスにおいては、当省から IX までのネットワーク稼働率をいう。
- 広域イーサネットサービスにおいては、広域イーサネットサービスのバックボーン内ネットワーク稼働率と○○省 WAN に接続される各拠点のアクセス回線ネットワーク稼働率をいう。
- 定義した稼働率は、1 か月に稼働すべき時間に対する実際に稼働した時間の割合であり、以下の計算方法で行うこととする。なお、稼働予定時間とは、原則として当該月の日数に 24（時間）をかけた時間数とし、累計停止時間とは、ネットワークに何らかの障害が発生し、データの送受信が行えない当該月当たりの累計時間数をいう。

  稼働率（%）＝（稼働予定時間 － 累計停止時間）÷ 稼働予定時間 × 100

(3) 障害の発生した時刻とは、受注者がネットワークの障害を検知した時刻、又は当省担当職員（以下「担当職員」という。）が受注者に障害を連絡した時刻のいずれか早い方とする。

(4) 障害の責任が受注者に帰するものでない場合及び計画的な工事、定期的な保守等に伴いネットワークを停止する場合は、稼働率の停止時間として扱わない。

(5) 運用を続けると障害に至ることが分かっていてネットワークを緊急停止する場合、緊急停止中の経過時間は稼働率の停止時間として扱うものとする。

(6) その他の SLA にかかる項目については、原則として、受注者のサービス約款に定める SLA に従うものとする。受注者は提案時にサービス約款に定める SLA を提出すること。

(7)回線冗長化などの対応により回線が停止中においても業務が継続できる場合は停止時間に含めない。

6.10.クラウドサービス

本項については、「4.8　クラウド利用者の立場からの考え方」を参照されたい。

6.11.クラウド構築

本項については、「4.9　クラウドを構築する立場からの考え方」を参照されたい。

6.12.セキュリティ

6.12.1.調達分野の定義

セキュリティに関しては、本章はこれまでの節とは異なり、各役務の調達におけるセキュリティ上の留意点を指す。

セキュリティの留意点は、情報システム調達に共通して留意すべき点、各調達分野の役務中のセキュリティに関する記述をそれぞれ記述している。

また、情報システムの構築時に、具体的なセキュリティの検討方法である「情報セキュリティを企画・設計段階から確保するための方策（SBD）」や「リスク要件リファレンスモデル（RM）分析のシステム設計」の活用に関して示している。

図　6.12-1　役務調達の分類における対応箇所

6.12.2.仕様書に共通して記載すべきセキュリティに関する留意点

6.12.2.1.情報システム調達に共通してセキュリティに関して留意すべき点

基本的に、各役務ドメイン共通で留意すべき点は、法令の遵守や基準、ポリシー、ガイドライン等の準拠となる。受注者は全ての作業において1～5に挙げている内容に留意する事が必要である。なお、応札の条件となる制約については、全て列挙する必要がある。また、準拠すべき基準、ポリシー、ガイドライン等は、応札中に応札者に開示される必要がある。

留意点	留意点の概要	記載するポイント
1. **政府機関の情報セキュリティのための統一基準の準拠**	「政府機関の情報セキュリティ対策のための統一基準」（情報セキュリティ政策会議決定）に準拠すること	「情報システムに係る政府調達の基本指針」に準拠して仕様書を作成している場合は、“セキュリティ要件”における記載の中で左記に準拠する旨を記載する
2. **各府省で定めるセキュリティポリシーの準拠**	上記「政府機関の情報セキュリティ対策のための統一基準」（情報セキュリティ政策会議決定）に準拠して各府省で策定している情報セキュリティポリシーに準拠すること	「情報システムに係る政府調達の基本指針」に準拠して仕様書を作成している場合は、“セキュリティ要件”における記載の中で左記に準拠する旨を記載する。 また、左記のポリシーが守秘義務締結後に省庁から公開される場合は、その旨も記載すること
3. **各種法令・規制等の遵守**	個人情報保護法、刑法、著作権法、不正アクセス禁止法等、当該の調達案件において関連する各種法令等を遵守すること	対象となる情報システム、業務が関連する法令・規制に関しては仕様書上で明記を行い、遵守する旨を記載すること
4. **その他ガイドラインの準拠**	1～3に記載した以外に、受注者に準拠又は対応を求めるべきガイドラインが存在する場合には、受注者は当該のガイドラインに準拠すること	情報システムの内容等から1～3以外に準拠するガイドラインを抽出し、仕様書に準拠又はガイドラインを実現する提案を求める旨を記載すること
5. **再委託先に対するセキュリティポリシー等の適用**	業務の一部を担当府省の承認を得て再委託する場合は、再委託を行う事業者にも受注者と同様の内容に準拠させること	一部業務について再委託先の活用が想定される場合には、再委託先にも受注者と同様の内容に準拠する必要があることを明記すること。

6.12.2.2.参照すべき基準・ガイドライン

「政府機関の情報セキュリティ対策のための統一基準（第4版）（平成21年度修正)」
(2010年5月11日情報セキュリティ政策会議決定)
http://www.nisc.go.jp/active/general/pdf/K303-091.pdf

6.12.3.情報セキュリティを企画・設計段階から確保するための方策（SBD）の活用

内閣官房情報セキュリティセンターでは、情報セキュリティ政策会議の要請を受け、経験・知見を有する有識者やベンダーを構成員とする「情報セキュリティを企画・設計段階から確保するための方策（SBD）に係る検討会（以下、「SBD 検討会」という。）」を設置・開催した。SBD 検討会においては、調達仕様の曖昧さによる情報システムの調達側と供給側双方における不利益の発生を軽減し、適切なセキュリティ対策を確実に実装することを目的とした「情報システムに係る政府機関におけるセキュリティ要件策定マニュアル」を策定予定である。

当マニュアルは、政府機関において「新規構築」及び「更改」を行う情報システムの調達全般を対象とし、特に情報システムの調達を担当する行政事務従事者が当マニュアルを活用してセキュリティ要件を自ら責任を持って策定し、調達仕様書に記載できることを期待している。また、情報システムを供給する事業者においても、当マニュアルを参照することによって、調達仕様書に記載されたセキュリティ要件の理解を助ける情報（策定過程に関する情報等）を得ることが期待できる。

セキュリティ要件の導出にあたっては、情報システムの情報保護のための対策及びセキュリティ侵害の対策を踏まえ、重要かつ効果的な要件を優先的かつ確実に調達仕様書に記載することで、必要に応じた適切なセキュリティ対策の確保を期待している。

6.12.3.1.セキュリティ要件導出の準備（システム概要図の作成及び要件詳細化）

マニュアルでは、まず、セキュリティ要件の導出に必要となる業務要件やシステム要件の導出手順を解説している。この手順において調達担当者は、調達予定の情報システムに関わる業務を洗い出し、業務ごとに主体、情報及び用いる環境を抽出してシステム概要図を作成する。その上で、作成したシステム概要図を踏まえ定型設問に回答することによって、業務要件やシステム要件を一定レベル以上の水準を確保した上で抽出する。

手順	概要
1. 目的及び業務内容の洗い出し	内部検討を行い、調達する情報システムの目的及び業務内容（業務の流れ、関連書類等）を整理する。
2. 業務に関わる主体の洗い出し	各業務の主体（人物、組織、情報システム等）を洗い出す。
3. 取り扱う情報の洗い出し	業務ごとに主体と取り扱う情報、その流れについて整理する。
4. 情報システム化する対象の決定	システム化の対象範囲を明確にする。他のシステムと連携する場合は、その関係も整理する。
5. 情報システム化する業務にて用いる環境の決定	各主体が対象システムを利用するにあたって、用いる環境（端末や回線等）を決定する。
6. システム概要図の作成	以上の結果から、一定の表記ルールに基づいてシステム概要図を作成する。
7. 定型設問による要件の詳細化	システム概要図を踏まえ、定型設問に回答する方法によって、対象システムの要件を「主体」「情報」「利用環境・手段」の 3 つの観点から詳細化する。

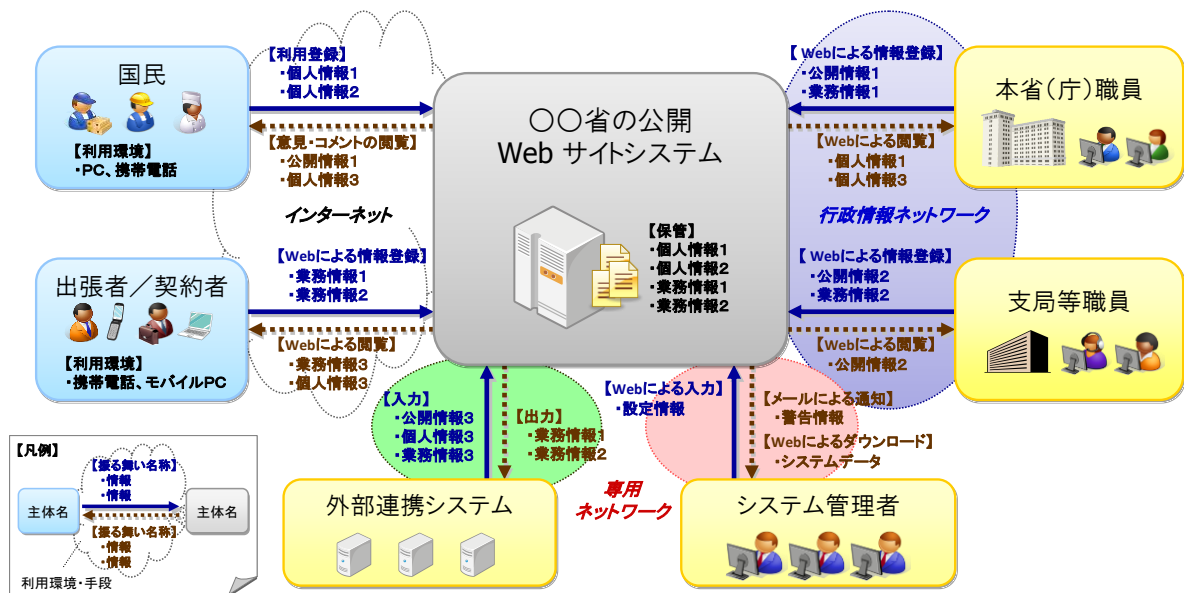



図 6.12-2 システム概要図の例

6.12.3.2.対策要件の決定

次に、上記での作業結果(整理した情報)を材料として、セキュリティ要件を導出する手順として、判断条件(優先的に実施することが望ましい対策要件を判断するための条件)による対策の方向性(対策方針)の検討、当該対策方針に対して合致する具体的な対策要件の決定方法を解説している。

手順	概要
1. 対策方針の検討	システム概要図及び定型設問によって抽出した要件に対して、判断条件を適用することによって、対策の方向性(優先的に実施すべき対策方針)を検討する。
2. 対応要件の決定	決定した対策方針に対して、コスト等に留意しつつ、合致する具体的な対策要件を決定する。
3. 調達仕様書への反映	以上の作業結果を調達仕様書に反映する。

6.12.3.3 その他

「情報システムに係る政府機関におけるセキュリティ要件策定マニュアル」では、上記にて抽出した要件で、具体的な対策要件に直結しないものの、応札する業者が提案(検討)のために活用しうると思われる情報(例えば、主体の規模等)を仕様書に記載する作業についても言及している。

さらに、対策要件に関する解説(対策要件の記載方法、想定脅威、実現例等)、統一基準の遵守事項と本マニュアルの対策要件の対応関係、作業実施にあたって参考となる関連文書等については、本マニュアルの別途付録に記載している。

以上、調達担当者(行政事務従事者)が自ら、調達する情報システムにおける適切なセキュリティ対策の実装の判断を行うためにも、本マニュアルを活用することが重要である。また、情報システムを供給する事業者においても、本マニュアルを参照することによって、調達仕様書に記載されたセキュリティ要件の理解を助

ける情報（策定過程に関する情報等）を得ることが期待できる。

6.12.4.リスク要件リファレンスモデル(RM)分析のシステム設計等への活用

6.12.4.1.「既存基準等」と「RM 設計要件」の関係と活用ポイント

RM で分析した、「組織業務への最終影響回避のための RM 設計対策要件」の各項目は、既存基準等のセキュリティ管理策に該当する具体的設計対策要件として関連付けられる。

この為、契約時の機能要件・試験要件として適用する事により、同時に既存基準等への契約上の準拠性が保たれることになる。

また、「組織業務への最終影響回避のための RM 設計対策要件」は「サイバー攻撃脅威モデル(攻撃シナリオ)」を定義する事により導き出した設計対策であるため、契約時試験におけるテストシナリオとして利用できる事を想定している。これにより、組織業務への最終影響回避に必要な機能の品質と脆弱性確認を絞って行う事が出来、コストパフォーマンス向上に繋がる。

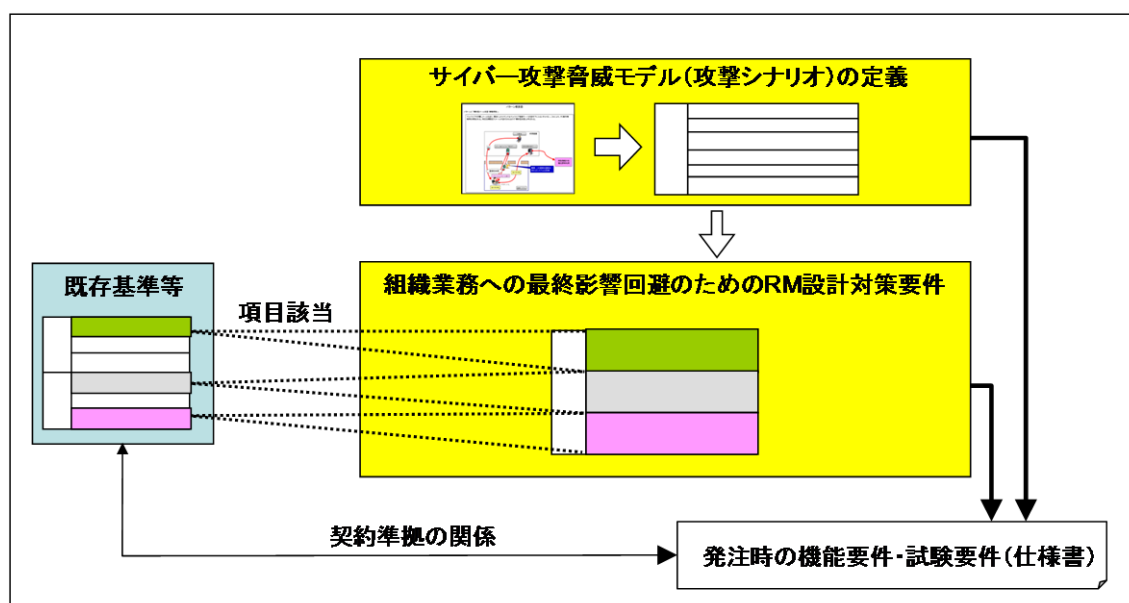



図 6.12-3 既存基準と RM 設計対策要件の関係

情報システムのセキュリティ対策に関する要件定義と構築の中で大きな問題となるのは、発注者や受注者等のシステムの関係者に対して、非機能要件であるセキュリティという専門性の高い分野で議論をしなくてはいけない事にある。

このため、RM は、発注者、受注者双方が情報システムのセキュリティ対策について共通の基準で検討するための枠組みを提供するものであり、各段階における、各関係者間で同一の問題認識に基づき具体的な対策実行要否及び設計機能の確定を狙いとしている。これにより、コスト見積及び要求精度の向上を意図する。

リスク要件リファレンスモデルの目的
リスク要件リファレンスモデルは、情報システムの発注者と受注者がそれぞれの立場で、具体的な脅威に基づいてシステムに組み込むべきセキュリティ対策を検討可能とするものとして開発された。本モデルによって、官公庁および民間の情報システム構築の発注者と受注者は共通の理解の下に情報システムに必要なセキュリティ対策設計が行われることを目的とする。

RM の検討に際し、前提としたシステム調達各段階におけるプロセスは以下である。

プロセス	実施内容	RM活用上のポイント
○システム発注時		
1.システム機能要求および諸条件の提示（発注者）	システム全体の運用要件の設定	
2.実現可能な具体的システム構成の検討（受注対象者）	システム全体の機能構成要件の設定	
3.脅威対象の特定と共有（発注者、受注対象者）	サイバー攻撃脅威モデル（攻撃シナリオ）の定義	RMサイバー攻撃脅威モデル（攻撃シナリオ）の活用
4.業務への影響把握と設計対策効果の理解（発注者、受注対象者）	サイバー攻撃脅威モデル（攻撃シナリオ）がシステム機能に及ぼす影響の理解	
5.システムへの対策事項の検討（発注者、受注対象者）	サイバー攻撃脅威モデル（攻撃シナリオ）がシステム機能に及ぼす影響の回避可能性を検討	受注対象者へ説明を要求し、発注者は確認
6.発注時の機能要件・試験要件（仕様書）の特定（発注者、受注対象者）	上記で確認された機能要件・試験要件を仕様書に記載	以下の活用 ・RMサイバー攻撃脅威モデル（攻撃シナリオ） ・組織業務への最終影響回避のためのRM設計対策要件」
○システム製造時		
7.システム設計、試験への展開	発注時プロセスで分析した結果を基に、システム基本設計、製造、試験等に展開	受注者は以下を実施 ・RM設計対策要件に基づく設計 ・攻撃シナリオに基づく関連脆弱性の是正と試験

なお、RM 検討時に前提とした標準的な運用手順は以下である。

リスク要件リファレンスモデルを用いてシステムを要求する発注者と具体的なシステムを提案し受注するシステムベンダーの間での標準的なやり取りの流れは以下の図のようなイメージで進められていく。このようなやり取りは、官民を問わず比較的規模が大きなシステムの設計時には通常実施されている流れの一部として組み込むことが可能である。

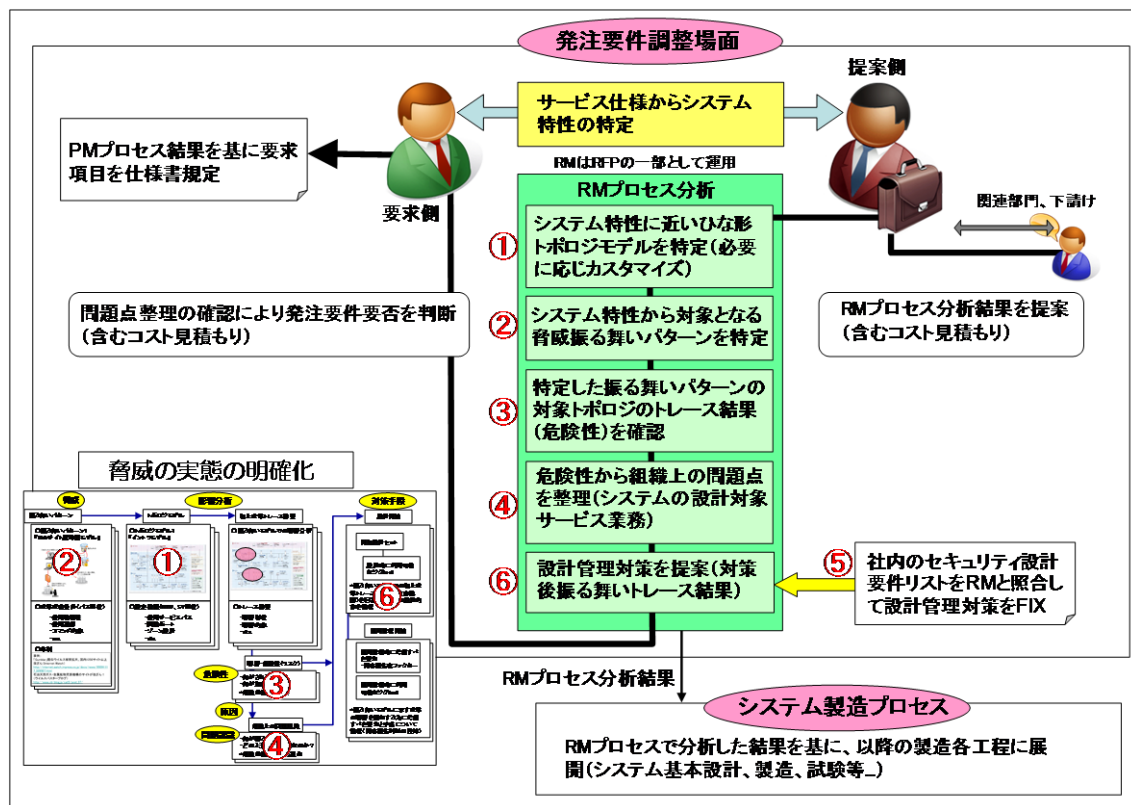



図 6.12-4 RMの標準運用手順

また、RM の応用として、本モデルを用いたインシデント発生時対処への活用を以下に示す。

リスク要件リファレンスモデルでは、脅威カタログとして、脅威対象のパターンとシステムトポロジのパターンが用意されている。この中では、それぞれの脅威対象がシステムの中でどのように振る舞い、どこで問題の現象が発現するかを把握する事はできるようになっている。したがって、既存のシステムに対してサイバー攻撃等を受けた際には、システムのどの部分で問題が発生していたかという事を特定し、その箇所に対する回避策等の暫定的な対策をシステムに講ずるための検討に用いる事ができる。

○攻撃情報入手時の自システム影響判断

サイバー攻撃事案発生時、自システムへの影響と回避策設計の有無、組織活動に与える影響の検討、暫定対策等の確認並びに対策立案に利用。

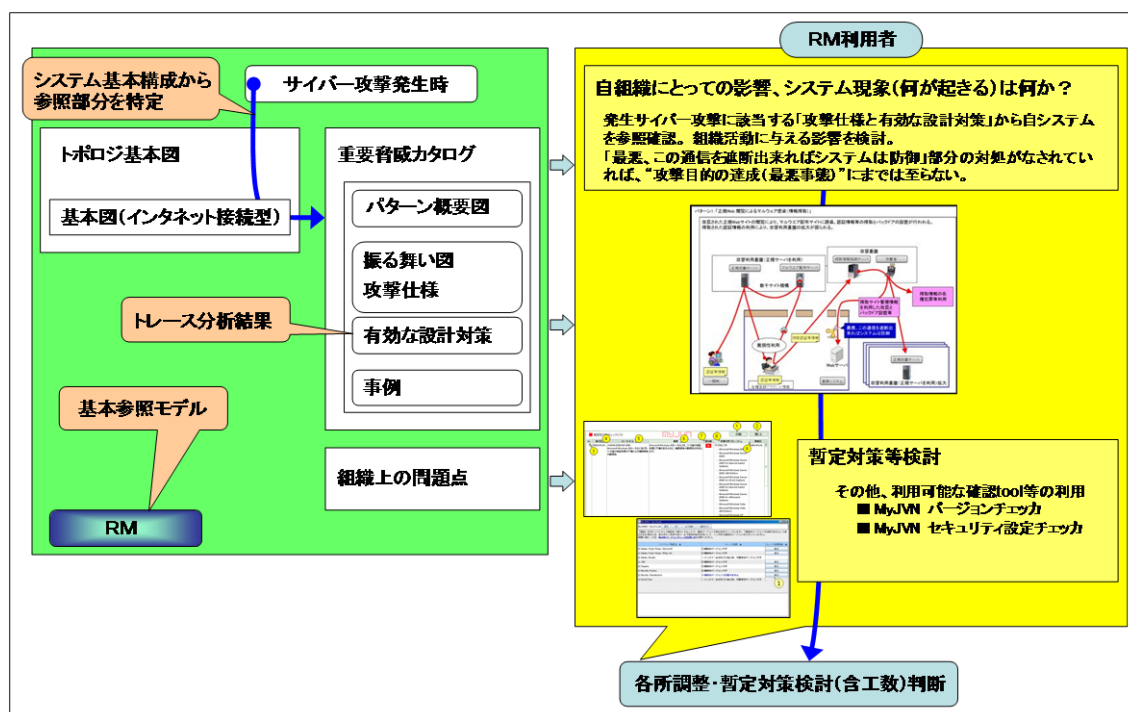



図 6.12-5 攻撃情報入手時の自システム影響判断への活用事例

6.12.4.2.RM 設計対策要件の導出の考え方

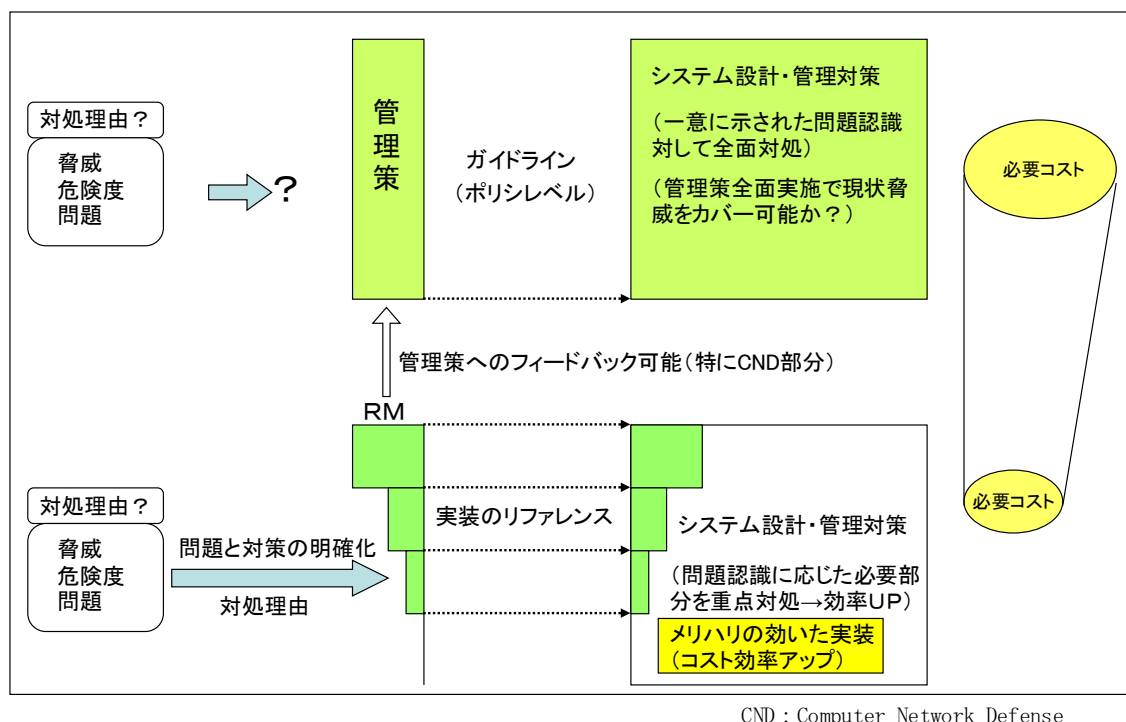
「リスク要件リファレンスモデル(RM)」は、これまで主要なセキュリティ対策と考えられてきた、セキュリティ製品を情報システム内に配置する設計手法が、標的型攻撃などの新たなサイバー攻撃手法の出現により、著しく有効性が低下していることが背景となっている。この状況を解決するため、現状のサイバー攻撃脅威の実態に基づき、業務への影響を評価し、必要とされる対策とコストを明らかにする手法として開発した。

CND : Computer Network Defense

図 6.12-6 RM のコスト効果

「リスク要件リファレンスモデル（RM）」の各分析コンポーネント（①～④）の概要を以下に示す。
なお、RM は組織の情報システムが受けるサイバー攻撃脅威を対象として分析したものであるが、仕様書にて実装を要求する場合は、サイバー攻撃によるミッションインパクトと投資効果を十分に検討して記載する必要がある。

① 現状のサイバー脅威の実像を具体的に分析整理した「攻撃パターン」を脅威モデルとして定義し、具体的な攻撃シナリオを整理。
② システムの各特性毎のシステムひな形として、情報システム設計モデルを設計。
③ 情報システム設計モデル上に攻撃パターンシナリオを攻撃トレース（机上模擬攻撃）する事により、影響と設計対策効果を分析。
④ 攻撃トレース（机上模擬攻撃）結果を「システム設計対策」として整理。

分析プロセス①：“現状のサイバー脅威の実像を具体的に分析整理した「攻撃パターン」を脅威モデルとして定義し、具体的な攻撃シナリオを整理。”

今日の脅威は、多様化・高度化・複雑化しているため、個別に対処を行っていたのでは、影響の分析や対策の立案が困難であり、契約段階や設計段階で対策を決定することは不可能である。このため、リスク要件リファレンスモデルでは、実際に確認された脅威の振る舞いを分析することにより、脅威を 6 つのパターンに分類し「重要脅威カタログ」として取りまとめ、これを分析したものを「攻撃パターン」として整理した。

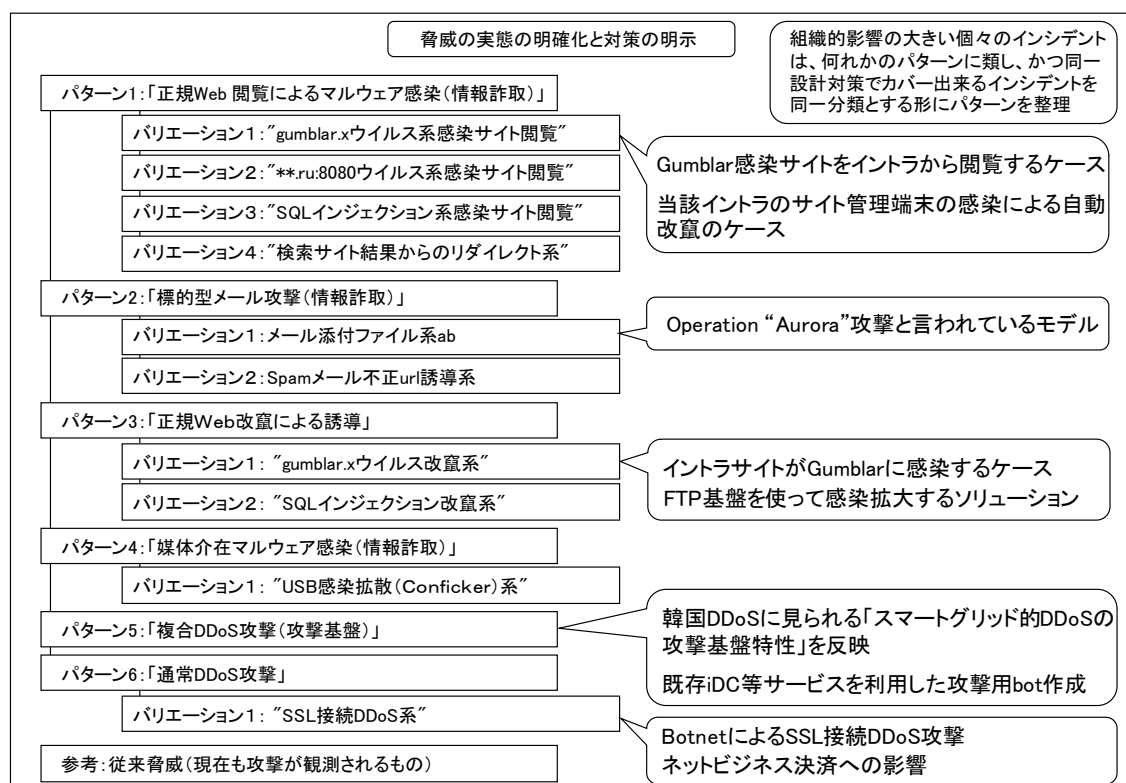



図 6.12-7 RMの対象とする攻撃パターン種別

各攻撃パターン概要を以下に示す。

「パターン 1:正規 Web 閲覧によるマルウェア感染(情報詐取)」

改ざんされた正規 Web サイトの閲覧により、マルウエア配布サイトに誘導。認証情報等の詐取とバックドアの設置が行われる。詐取された認証情報の利用により、攻撃利用基盤の拡大が図られる。
自システム内ユーザが、改ざん正規サイトを閲覧し、マルウエアに感染するケースが該当する。

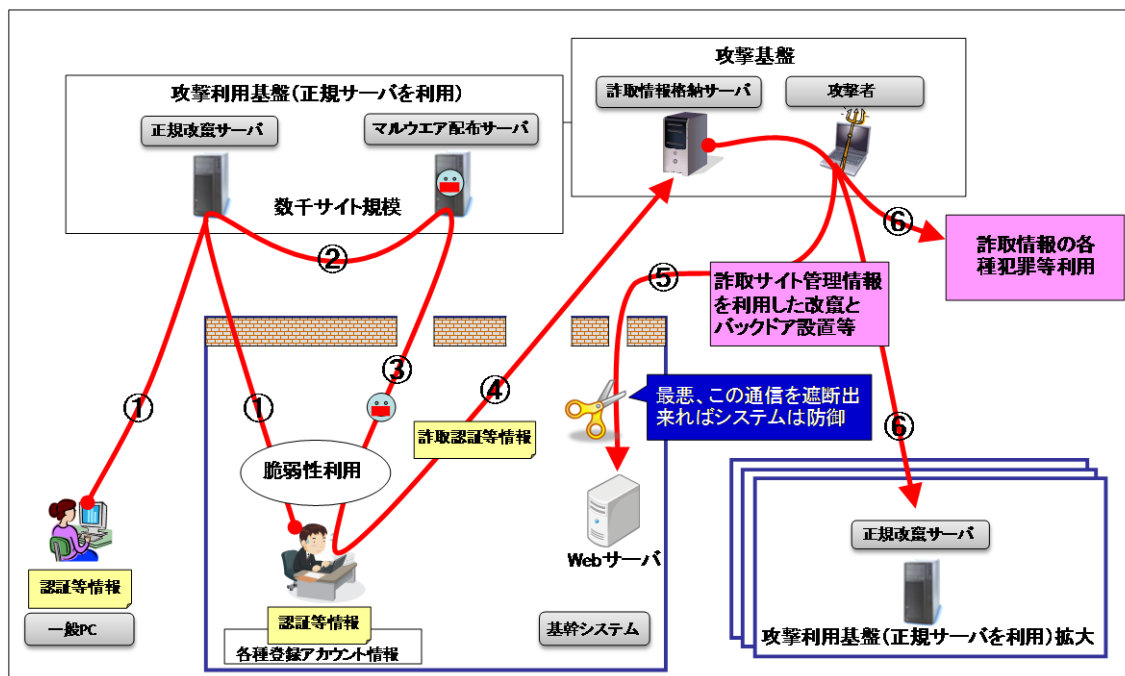



図 6.12-8 パターン1:「正規 Web 閲覧によるマルウエア感染(情報詐取)

「パターン 2:標的型メール攻撃(情報詐取)」

大量のユーザを無差別に狙うのではなく、特定の組織や企業に属している個人を標的とし、タイトルや文面、送信者名を偽ってマルウエア付きメールを送る攻撃。

開封によりマルウエアが実行され、システムの Bot 化や組織情報の詐取が行われる。特定組織目標限定でメールが送付されるので「標的型攻撃」と呼ばれる。

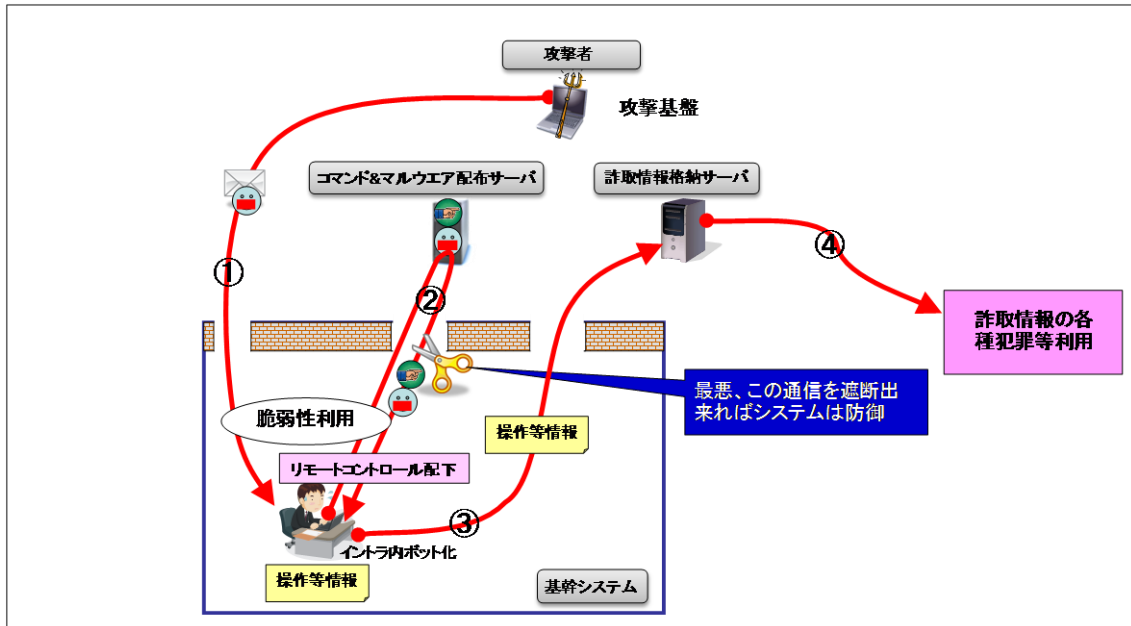



図 6.12-9 パターン 2:「標的型メール攻撃(情報詐取)」

「パターン 3:正規Web改ざんによる誘導」

　サイト閲覧者をマルウエア配布サイトに誘導するため正規 Web サイトを改ざんする。

自システムの Web サイトが改ざん(リンクの挿入)され、外部閲覧者のマルウエア配布サイトへの誘導に利用されるケースが該当する。

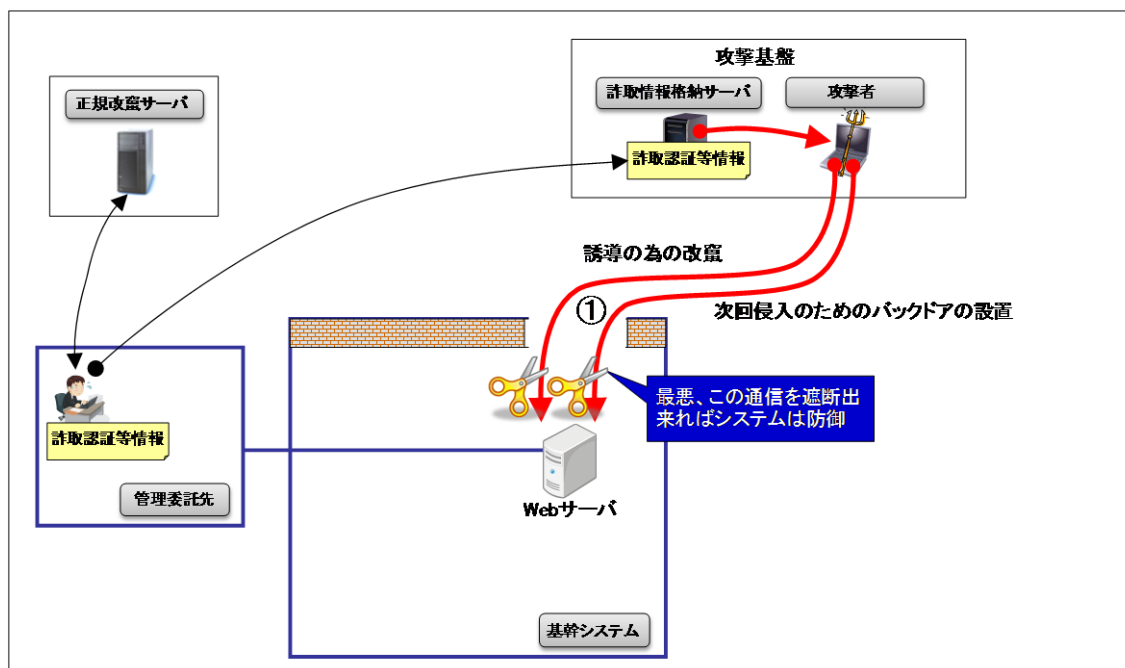



図　6.12-10 パターン 3:「正規Web改ざんによる誘導」

「パターン 4:媒体介在マルウェア感染(情報詐取)」

製品開発ライン等種々の場面で媒体等に混入したウイルスが USB 等媒体を介してシステムに侵入。侵入後、攻撃利用基盤上のマルウエアにアップデート。同時に、基幹システム内へのネットワーク感染及び媒体を介して感染拡大を図る。

ネットワーク障害、サーバ障害双方に跨る影響現象が発生するため、両管理組織間とセキュリティ部門との連携と切り分け手順等の準備が効果的。

システムに侵入したマルウエアは、システムに侵入口(バックドア)を設置し、システム情報詐取を行う。

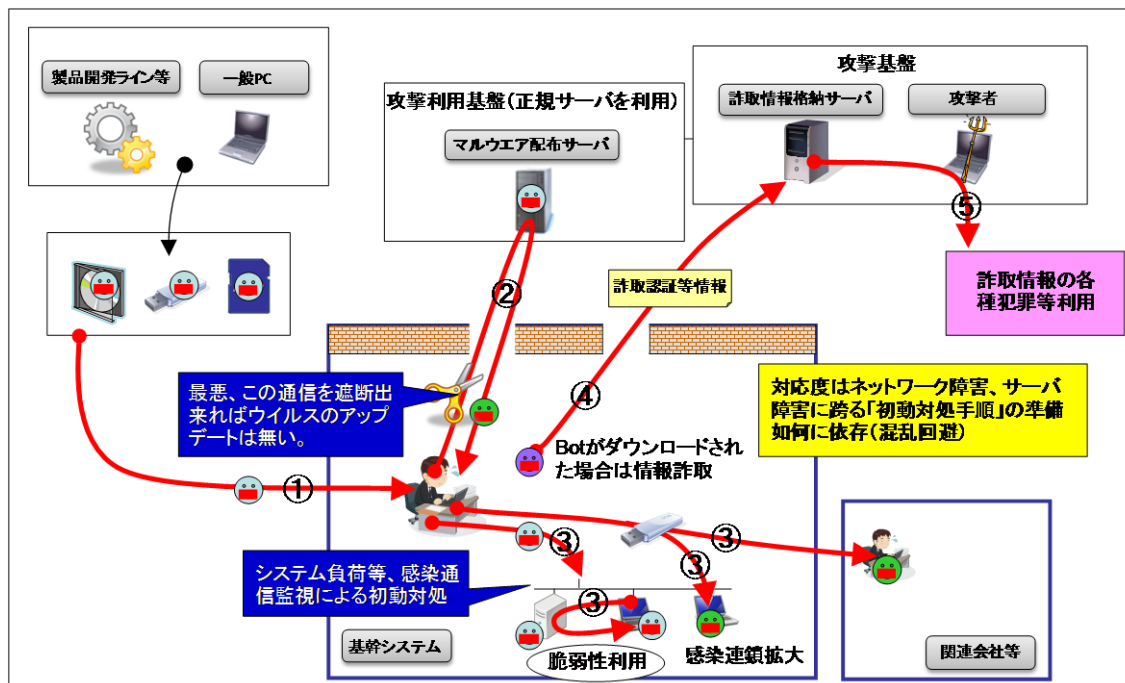



図 6.12-11 パターン 4:「媒体介在マルウェア感染(情報詐取)」

「パターン 5:複合 DDoS 攻撃(攻撃基盤)」

マルウェアに感染したPCが、 Web サーバに対して DDoS 攻撃を実施しつつ、悪意のあるサーバから攻撃指示情報や他のマルウェアをダウンロードし、マルウェアに感染した PC において大量スパムメール送信やファイル破壊を行う。

複合型の DDoS は、従来安全性を担保する前提で構築された既存サービス網(VPN 網)の使用や機能分散されたそれぞれのマルウエアが連動して攻撃機能を発揮するなど、攻撃利用基盤構築に関して新しいタイプの攻撃。防御情報の分析が困難なため、今後多用な攻撃に利用され始めると対応の難しい脅威となる。

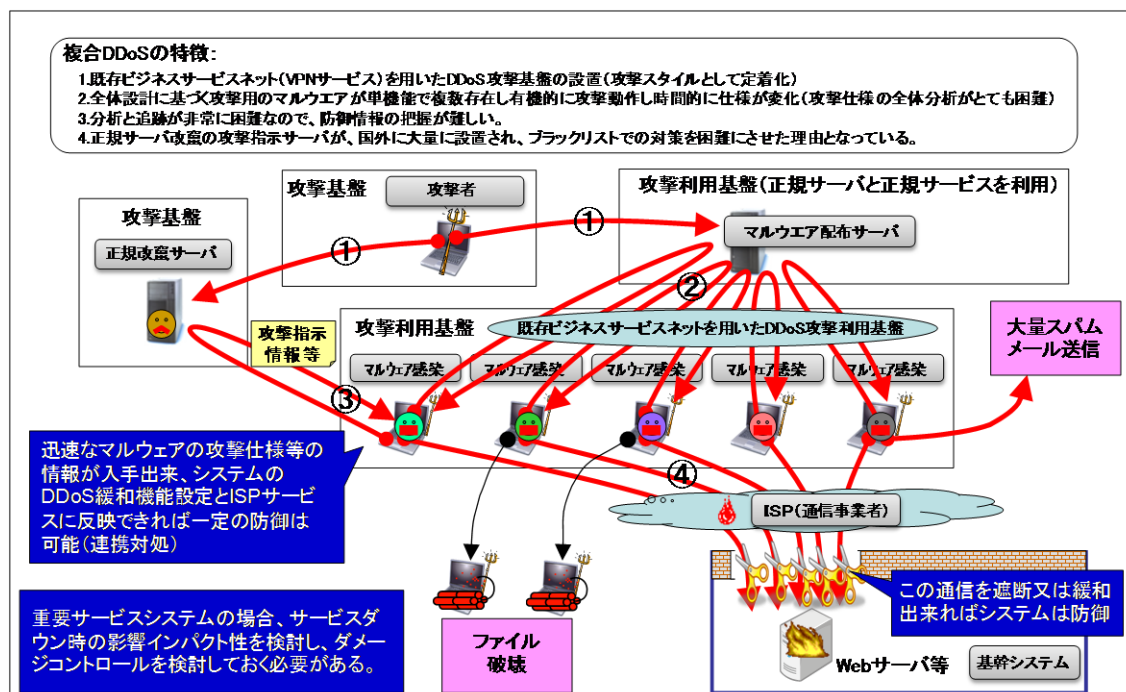



図 6.12-12 パターン 5:「複合 DDoS 攻撃(攻撃基盤)」

「パターン 6:通常 DDoS 攻撃」

ネット決済サイトビジネスへの DDoS により、販売決済が不能。ビジネスへの影響が発生するが、対応策検討にはビジネスインパクトと対策コストとの総合判断が必要。

回線の過負荷を引き起こす DDoS(回線帯域系 DoS)の場合は、サイト側対応での防御が出来ないため、契約内容含めた回線側との対応調整が必要。この場合もコスト対効果を勘案しつつの検討になる。

処理負荷加系 DoS の場合は、サイト側の DoS 緩和機能の設定による回避を行うが、この場合設定に必要な攻撃分析情報を入手する必要があり。この為の組織ラインを確保しておく必要がある。SSL 接続 DoS 攻撃の場合、SSL サイトにアクセスできない。

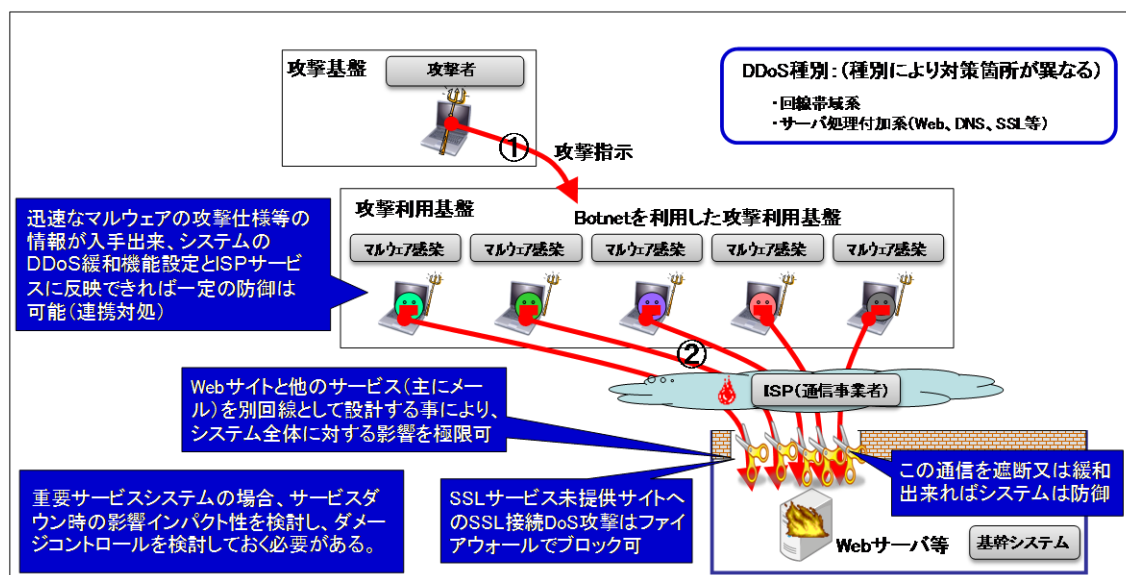



図 6.12-13 パターン 6:「通常 DDoS 攻撃」

さらに各振る舞いパターン1〜4から、組織業務への最終影響に係わる部分の共通部分を抽出整理したものが下記「戦術的な攻撃の基本モデル」であり、「サイバー攻撃脅威モデル(情報詐取攻撃シナリオ)定義の基礎」となっている。

第1段階:システムへの初期潜入

様々な手法によるシステムへの初期マルウエアの投入。マルウエアは非常に多種に渡り、脆弱性パッチの存在しない脆弱性(ゼロデイ脆弱性)やアンチウイルスパターン未適用のマルウエアも多様され、正規通信(HTTP、SMTP)で投入されるため、FW、アンチウイルスパターン、脆弱性パッチ等の従来対策での第1段階防御には限界がある。

第2段階:マルウエアダウンロードサーバへの接続と攻撃マルウエアの投入

外部のマルウエアダウンロードサーバに接続しマルウエアのアップデート、攻撃指示等の受信を行う。この際の通信は、HTTP、SSL 等が用いられた正常通信であるため、FW,IDS 等での検知遮断は行われない。第2段階攻撃は発見しにくく攻撃に気がつかないケースも多い。

第3段階：情報詐取と攻撃指示の継続

攻撃者のリモート指示に基づき、攻撃の最終目的である「情報詐取」を行い、情報を外部に送信する。

この際の通信は、HTTP、SSL 等が用いられた正常通信であるため、FW,IDS 等での検知遮断は行われない。第3段階攻撃は発見しにくく攻撃に気がつかないケースも多い。

組織にとっての最終脅威（問題）は、この第3段階に攻撃に存在する。

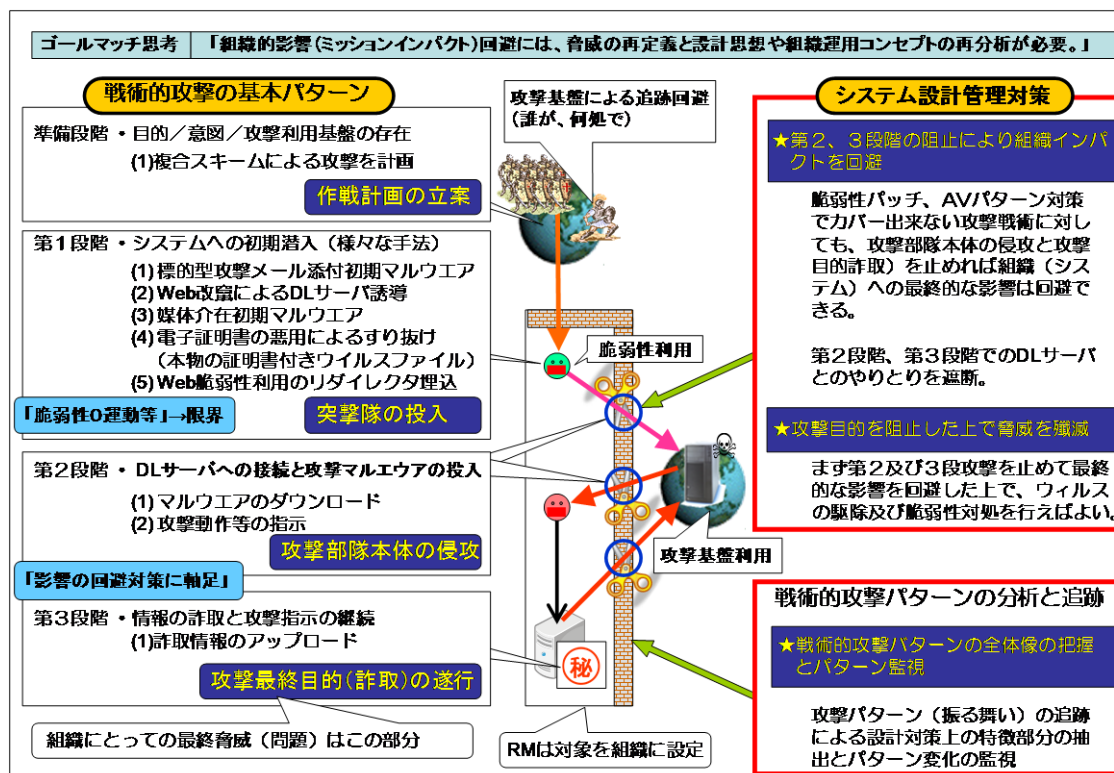



図 6.12-14 サイバー攻撃の共通基本モデル

分析プロセス②：“システムの各特性毎のシステムひな形として、情報システム設計モデルを設計。”

情報システムが攻撃を受けた際の脅威（ウイルス等）の振る舞いを分析するため、典型的な情報システムの構成例を４つの「システムトポロジーモデル」として整理した。

各システムトポロジーモデルは、必ずしも単独で利用されるわけではなく、たとえば「イントラネットモデル」と「iDC モデル」の組み合わせなど、複数のモデルを組み合わせることも念頭に置いている。

A イントラネットモデル B 閉域型モデル C iDC モデル D SaaS モデル

以下に、イントラネットモデルの例を示す。

No	モデル名	システムトポロジモデルの概要と特徴
1	イントラネットモデル	・ 官公庁、民間の情報システムで最も多い情報システムの構成である。 ・ イントラネット内を外部向けウェブサーバなどを設置するDMZ(DeMilitarized Zone)と外部からの直接アクセスを許さない構内システムエリアに分けて運用する。 ・ 外部公開 Web サーバ等 DMZ エリア部分のみを iDC に設置して運用するシステム形態もイントラネットモデルに含む ・ 支所、支社、出張所などの小規模拠点では DMZ を経由せず、各所の構内システムから直接インターネットアクセスを行う構成をとっているケースがあるが、そのような構成もイントラネットモデルに含む。
2	閉域型モデル	・ 医療情報システム、製造業の FA システムに比較的多く見られる構成であり、情報システムが構内で完結しており、外部のインターネットとの接続を持たないシステムを指す。 ・ インターネット接続を持たないため、ネット経由のサイバー攻撃を受けることはないが、アンチウイルスソフトのパターン更新がなされない･更新タイミングが遅れる等のため、ウイルス汚染された USB メモリ、CD などが持ち込まれた場合に被害が広がりやすい。
3	iDC モデル	・ iDC の利用形態は様々であるが、ここでいう iDC モデルは、業務システムまでを含めて iDC 上で運営しているケースを想定している。 ・ 外部向け Web サーバなど DMZ 部分のみを iDC に置くケースはイントラネットモデルで扱うことができる。一部の業務システムを iDC で運用し、その他を自社イントラネットで運用している場合は、イントラネットモデルと iDC モデルの組み合わせによって扱うことが可能である。 ・ スイッチやサーバを他の iDC ユーザと共有することの影響や iDC 側の管理端末が複数の iDC ユーザのシステムにアクセスすることの影響があることがイントラネットモデルと異なるところである。
4	SaaS モデル	・ SaaS では、ユーザは契約したサービスをインターネット経由で利用するのみであり、サーバや DB 等のシステムリソース管理は一切行わない。 ・ ユーザ側が SaaS 利用に関して行えるセキュリティ対策はアクセス管理のみであり、他のセキュリティ対策は全て SaaS 提供事業者に委ねることになる。この点が、iDC を利用した

No	モデル名	システムトポロジモデルの概要と特徴
		システム運用とも異なるものである。

分析プロセス③："情報システム設計モデル上に攻撃パターンシナリオを攻撃トレース(机上模擬攻撃)する事により、影響と設計対策効果を分析。"

「振る舞いモデル」で作成した「振る舞いパターン(攻撃シーケンス及び攻撃仕様)」の、各「システムトポロジーモデル」上での影響動作を分析するための「脅威トレース」(机上模擬攻撃)により、トポロジー上に実装されたセキュリティ対策の効果を評価し、脅威を抑止するための技術的な手法をベストプラクティクスとして検討した。また、「脅威トレース」は、実攻撃事案の発生状況に即した状態で行った。

分析プロセス④："攻撃トレース(机上模擬攻撃)結果を「システム設計対策」として整理。"

「脅威トレース」(机上模擬攻撃)で明らかになった効果の高い設計対策を各振る舞いパターン毎の「システム設計対策」として整理した。

以上の分析から、昨今の攻撃モデルは、組織業務への最終影響に係わる部分は一部の攻撃手法を除き、共通の攻撃仕様となっており、システムトポロジ形態や攻撃振る舞いパターンに依存しない事が判る。これは攻撃目的が変遷し同一となって来ている為だと思われる。

このため、「共通的な攻撃シナリオと設計対策」を導きだし、以下に整理した。

〇サイバー攻撃脅威モデル(攻撃シナリオ)の定義

〇組織業務への最終影響回避のための RM 設計対策要件(仕様要件集)

6.12.4.3.サイバー攻撃脅威モデル(攻撃シナリオ)の定義

従来の設計対策は、第1段階を重点に考えられた攻撃ストーリを前提にしてきたが、その対策工数や効果も限界となってきてる。

一方、昨今の情報詐取を目的としたサイバー攻撃における共通的なサイバー攻撃脅威モデル(攻撃シナリオ)は、第1～3段階のプロセスを踏んでおり、特に組織(業務)に影響が大きいのは外部アクセスを伴う第2,3段階である。

このため、従来対策とは別に、現状種々のサイバー攻撃事案の分析を基に、組織にとっての最終影響問題に該当する攻撃脅威を攻撃目的に直結する第2，3段階攻撃部分とし、各種攻撃パターン共通の攻撃モデルとして下記の2種に設定した。

〇「情報詐取攻撃(サイトへのリダイレクトリンク埋込改ざん含む)」

〇「サービスの妨害・停止攻撃」

```
攻撃目的
|
+---01_情報詐取攻撃
| +---パターン1:「正規Web 閲覧によるマルウェア感染（情報詐取）」
| | +---バリエーション１:gumblar.xウイルス系感染サイト閲覧
| | +---バリエーション２:.ru8080ウイルス系感染サイト閲覧
| | +---バリエーション３:SQLインジェクション系感染サイト閲覧
| | +---バリエーション４:検索サイト結果からのリダイレクト系
| +---パターン2:「標的型メール攻撃（情報詐取）」
| | +---バリエーション１:メール添付ファイル系ab
| | +---バリエーション２:Spamメール不正url誘導系
| +---パターン3:「正規Web改竄による誘導」
| | +---バリエーション１: gumblar.xウイルス改竄系
| | +---バリエーション２: SQLインジェクション改竄系
| +---パターン4:「媒体介在マルウェア感染（情報詐取）」
|   +---バリエーション１: USB感染拡散（Conficker）系
|
+---02_サービスの妨害・停止攻撃
| +---パターン5:「複合DDoS攻撃（攻撃基盤）」
| +---パターン6:「通常DDoS攻撃」
|   +---バリエーション１: SSL接続DDoS系
|
+---従来脅威（現在も攻撃が観測されるもの）
```

以上を考慮し、サイバー攻撃脅威モデル（攻撃シナリオ）を以下に定義する。
また、本シナリオは「試験要件」としても活用する事を想定している。

「情報詐取攻撃（サイトへのリダイレクトリンク埋込改竄含む）」の攻撃シナリオ		
第１段階プロセス 「システムへの初期潜入」	手法1	①認証等情報を保持している一般PCが、改竄されている正規Webサイトを閲覧し、一般PC内のソフトウェアの脆弱性を悪用して、マルウェア配布サイトにリダイレクトされる。→以後、第2段階プロセスが実施される。
	手法2	①攻撃者が、イントラ内の一般PCに対して悪意のある偽証メールを送付。 ②一般PCにおいて、偽証メールの添付ファイルを開く事によりマルウェアが実行される。→以後、第2段階プロセスが実施される。
	手法3	①別途取得されたftp ID/PWにより、外部から自Webサイトの改竄がなされる。 ②自Webサイトにマルウエア配布サーバへのリダイレクト埋め込み（改竄）がなされる。
	手法4	①USBメモリ等の電子記憶媒体に混入したマルウェアが、その媒体を介して一般PCに混入する。 ②記憶媒体、ファイル共有及び脆弱性を利用したネットワーク感染により、初期感染PCから他の一般PCに対してマルウェア感染を拡大 。 ③一般PCに混入したマルウェアが脆弱性を利用して実行される。→以後、第2段階プロセスが実施される。 注:オープン～クローズ系間でUSB等によるファイル移管運用がある場合は、クローズ系もオープン系と同様の攻撃シナリオが適応される。

「情報詐取攻撃（サイトへのリダイレクトリンク埋込改竄含む）」の攻撃シナリオ		
第2段階プロセス 「マルウエアダウンロードサーバへの接続と攻撃マルウエアの投入」	手法1	①外部のサーバ（コマンド＆マルウェア配布サーバ）に対して通信を行い、更新マルウエアの機能更新や別のマルウェアがダウンロードされる。 注：外部サーバは、乗っ取られた正規サイト（攻撃基盤上）を利用される。 注：外部サーバは、随時変更され特定アドレスの遮断は無効。 注：外部のサーバとの通信はHTTP,SSL等の正規サービスメッソドを利用するため、FWでの検知・遮断は出来ない。
	手法2	①認証等情報を保持している一般PCが、改竄されている正規Webサイトを閲覧し、一般PC内のソフトウェアの脆弱性を悪用して、マルウェア配布サイトにリダイレクトされ、マルウェアをダウンロードさせる。

「情報詐取攻撃（サイトへのリダイレクトリンク埋込改竄含む）」の攻撃シナリオ		
第3段階プロセス 「情報の詐取と攻撃指示の継続」	手法1	①外部のサーバ（コマンド＆マルウェア配布サーバ）から、マルウエアに対して、攻撃動作等の指示を行う。 注：攻撃等指示は、多くの固有コマンドを持っており動作の解明は困難。 注：外部サーバは、乗っ取られた正規サイト（攻撃基盤上）を利用される。 注：外部サーバは、随時変更され特定アドレスの遮断は無効。 注：外部のサーバとの通信はHTTP,SSL等の正規サービスメッソドを利用するため、FWでの検知・遮断は出来ない。
	手法2	①ダウンロードされたマルウェアが、認証等情報を不正に詐取し、外部のサーバに送信する。 注：外部サーバは、乗っ取られた正規サイト（攻撃基盤上）を利用される。 注：外部サーバは、随時変更され特定アドレスの遮断は無効。 注：外部のサーバとの通信はHTTP,SSL等の正規サービスメッソドを利用するため、FWでの検知・遮断は出来ない。

「サービスの妨害・停止攻撃」の攻撃シナリオ		
攻撃プロセス	手法1	注：複合的な攻撃基盤により正規PC等から、DDoS攻撃仕様が柔軟に変化する攻撃がなされる事により、攻撃元等の攻撃解析が困難である事を前提とする。 ①DDoS攻撃以外に大量スパムメール送信や、感染したPC内部のファイル破壊を実施する。（DDoS攻撃以外は、情報詐取攻撃シナリオに同じ）
	手法2	②DDoStool等利用によるDDoS攻撃。攻撃内容は以下のとおり。 ・安易なFTP PW設定サイトの捜索（FTPブルートフォース）とアジサイト改竄 ・ SQLインジェクション脆弱性サイト捜索とアジサイト改竄 ・他国proxyサイト利用によるDDoS（国別IPフィルター対処不能） ・多数の偽証IPによるDDoS（IPフィルター対処不能） ・帯域DDoSと負荷DDoSの併用

6.12.4.4.組織業務への最終影響回避のための RM 設計対策要件

従来、第1段階の攻撃手法に対し「境界防衛」の考え方による設計がなされてきたが、昨今主流の多段型攻撃においては、その対策効果に限界が生じており、第1段階攻撃は突破される事が多い。

このため、共通的なサイバー攻撃脅威モデル（攻撃シナリオ）における第1段階の攻撃手法に対する設計対策とは別に、組織業務への影響が大きい第2、3段階への対策を重視し「組織業務への最終影響回避の為の設計対策要件（非機能要件を含む）」を検討した。

情報詐取攻撃においては、第2、3段階の攻撃手法は事案において共通的である事から各攻撃共通的な設計対策要件が案出可能である。また、クローズ系システムにおいても、USB 等媒体を介してクローズ系脅威と同等脅威と考えられる事案が発生しており、今後多用される攻撃技術と考えられる事から、システムトポロジに係わらず共通的な設計対策として定義する。

また、DDoS 攻撃においては背景や目的は様々で、これに応じた攻撃手段も種々存在するが被攻撃システム側から見た攻撃通信は同種である。

これらを考慮し、2種別の攻撃シナリオに応じた「最終影響回避の為の設計対策要件(運用管理等非機能要件を含む)」及び「システム設計の設計前提としての運用条件」を以下に定義する。

	機能要件項目	機能要件内容	要件理由及び背景	設計事例
1	2要素認証・ワンタイムパスワードの導入	Webサイト更新用fto iD/PWに加えワンタイムパスワード(OTP)等を併用する2要素認証の使用。	Webサイト管理のftp ID/PWが漏出した場合の認証強化。 ・Gumblar事案等対処事例	・ワンタイムパスワード(OTP)
2	「管理用LAN」の設定	サーバ管理用の外部に公開しない構内ネットワークを設定(裏側LAN)。	マルウェアに感染したクライアントPCがサーバ管理用端末であった場合、管理者用FTPのIDやパスワードが攻撃者に渡ってしまう場合がある。 そのような場合でも、Webサーバの更新を管理用LAN(裏側LAN)経由に限定しておくことで、WebページにJavaScriptを埋め込まれる被害は防ぐことができる。 ・Gumblar事案等対処事例	・ネットワークトポロジ設計
3	Webサーバ管理端末のアクセス先制限	Webサーバの管理端末のソフトウェアアップデート等特定のサイト以外へのアクセスを禁止に設定。	正規サイトのアクセスのみでクライアントPCがマルウェアに感染するため、管理端末のアクセス先制限により、マルウェア感染確率が低下し、管理者のFTPアカウントなどの重要データを盗み出される可能性が低下する。	・管理用端末設定 ・システムプロキシ設定
4	プロキシの認証情報のチェック	一般PCの外部Webアクセス時、認証プロキシによる認証アクセスを設計。	マルウェアが、独自の通信メソッドを用いて詐取した情報を悪性サイトに送信する場合、認証情報を使用しない場合が多いことが確認されている。 ・マルウエアが既認証状態を使用した攻撃仕様となった場合は、防止出来ない。	・認証プロキシ

5	システムプロキシ経由通信コントロール	一般PCの外部Webアクセス時、システムプロキシを介した外部アクセスを設計。 ファイアウォール等により、特定ポートの通信でプロキシを経由しない(グローバルIP)外向き通信の遮断。	マルウェアが、詐取した情報を悪性サイトに送信(盗み出し)する場合、80,443ポートを使い独自の通信メソッドを用いるケースが多いことが確認されている。これらの通信の多くはシステムプロキシを使用していない。 また、外部ホストへの接続試行通信にグローバルIPを用いるマルウエアはFWリールで遮断可能。 ・システムプロキシの設定を利用して通信するマルウエアには無効	・システムプロキシ設定 ・FWルール設定
6	HTTP,SSL通信のヘッダーチェック	HTTP,SSL通信のヘッダー等(GET,POSTコマンド)内容の検出・遮断。	マルウェアが窃取した情報を外部の悪性サイトに送付する場合、新たな攻撃コードをダウンロードする場合、C&Cサーバからの指示を受信する場合に多くは80/tcp,443/tcpが用いられる。 また、HTTP通信の場合の通信ヘッダー(メソッド)が通常使われるRFC標準プロトコルからはずれていることが確認されている。	・
7	侵入検知(IDS)機能の活用(マルウエアダウンロード検知)	IDS,IPSによる外部悪性サーバとの他マルウエアやアップデートのダウンロード検知(イン/アウト)。	IDS(IPS)は未登録シグネチャを持つ不正通信は検知することができない。 IDSの有効性を高めるためにはSOC(Security Operation Center)運用と一対となった運用を行い、 通常の通信パターンと異なる通信の検出等の独自シグネチャのタイムリーな更新が不可欠。 ・ただし、規定シグネチャでは無いためSOCの運用能力に依存。	・IDS,IPS(SOC運用含む)

8	未知のウィルス検出ソフトウェアの導入	ゼロデイ脆弱性含む、マルウエアが脆弱性を使用した時の挙動検知。	PC上のウィルスの脆弱性利用等の挙動などから攻撃動作を検出することにより、未知ウイルスや、未知の脆弱性を突く「ゼロデイ攻撃」を検出し防御することが可能な製品が複数の企業から発表されてきている。 ・従来のウィルス対策ソフトを補完するものとして、防御機能、管理工数等十分な評価の上で設計利用検討の可能性がある。	・脆弱性使用検知
9	ルータ等でのルーティング設定	ルータ、SWによる必要なアクセス範囲に限定した、VLAN及びルーティング設定。	システムへの影響を最小化するため、攻撃時の影響範囲をネットワークトポロジ設計上分離する。 ・Conficker、stuxnet事案等対処事例	・ネットワークトポロジ設計 ・ルータ、SWのVLAN設定
10	容量負荷監視による感染動作の検出	ファイルSV、SWの負荷及びログ等容量監視によるネットワーク感染動作の検出。 ネットワーク及びシステム監視管理機能の異常負荷検知機能の設計。	マルウエアがシステム内ネットワーク感染を拡大する場合、ネットワークトラフィック異常で検知できる。 このため、ネットワーク管理部署との連携により、各箇所の要領監視による発見監視とルータ等箇所での一時通信遮断等運用による対処が有効となる。	・ネットワーク監視機能、運用

「サービスの妨害・停止攻撃」の設計対策要件（運用管理等非機能要件を含む）

	機能要件項目	機能要件内容	要件理由及び背景	設計事例
1	DDoS緩和機能	FW,バランサ等のDDoS緩和機能の設定による処理負荷上昇型DDoSへの対応 DDoS緩和装置の導入検討	FW、バランサにはDDoS緩和機能を保有しており、DDoS攻撃通信の内容により、本機能の再設定により処理負荷上昇型DDoSの影響が緩和される。 さらに効果を期待するためには、学習した通常の通信トラフィックパターンから逸脱した通信を検知した場合に、DDos対策装置にアラートを発し、帯域制御、アクセス制御を行うDDos対策専用装置の導入を必要に応じ検討。 ・DDoS攻撃手段、通信内容等の分析組織等との連携が必要。	・FW、バランサのDDoS緩和機能の設定 ・DDoS緩和装置
2	ISP事業者によるDDos対策サービスの活用	回線帯域負荷上昇型DDoS対応のためのISP事業者との契約等検討	DDos攻撃は、攻撃を検知できたとしても大規模なものに対しては単独では防御が困難な場合が多い。 ISP事業者が自社の強力なバックボーンを使ったDDos対策サービスを提供しており、必要に応じこれらの活用も検討する。	・DDos対策サービスの利用

システム設計の設計前提としての運用条件

1	設計前提としての攻撃被害対応時体制	現状のサイバー脅威の攻撃動作分析と攻撃パターンの分析から、サイバー攻撃が高度化していることが明らかになっている。 このため、ユーザーのシステム部門だけで攻撃の内容を分析し、適切な復旧対策をたてることは非常に難しくなっている。 設計時の運用体制設計に、セキュリティベンダーやSIerとの連絡、協力体制を組み込み、攻撃を受けた際の対応、責任分担を明確にしておくことが攻撃対処の前提となる。
2	感染通信ポートの遮断等「初動対処オペレーション手順等の準備」	拠点ルータでの感染通信ポートの遮断や一時切り離し等による封じ込めによるシステム内での感染拡大を押さえ込むための「初動対処オペレーション手順等の準備」 ＊手順の準備及び運用管理如何により、対処速度に差が発生。 ・ルータ、SWにおけるネット感染portの閉鎖手順 ・ネットワーク障害、サーバ障害を総合的に把握し切り離し部分の事前検討等 ・ファイルSV、SWの負荷及びログ等容量監視での検知手順

6.12.5.各調達分野の役務中のセキュリティに関する記述

各調達分野の TRM の役務の中に、調達分野ごとに記載すべきセキュリティの役務要件が盛り込まれている。各調達分野において記載されているセキュリティにおいて留意すべき点とその概要について以下に示す。実際の調達を行う場合には下記のリストに記載されている留意点に関して検討がなされているかをチェックする必要がある。

●6.2.調達支援

留意点	留意点の概要	TRM での記載箇所
情報セキュリティ要件の定義	発注者及び仕様書作成者は、「政府機関の情報セキュリティ対策のための統一基準」、及び各府省の情報セキュリティポリシーに準拠して、情報セキュリティ要件の定義を行うこと。 特に以下の要件に関しては、「情報システムに係る政府調達の基本指針」において仕様書への記載が求められている事から、特に明確に定義を行うこと （１）権限管理の定義 （２）セキュリティ対策の定義 「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む）及びアクセス制御における許可情報を管理することをいう。	6.2.調達支援 2. 要件定義の支援

●6.3.システム構築（設計･開発） ※6.3-1～6.3-4 共通

役務項目	役務の概要	TRM での記載箇所
開発環境のセキュリティ対策	開発に係わる環境（機器、作業室等）を受注者側が用意する場合には、これらの環境に対しても充分な情報セキュリティ対策を実施すること	開発環境の準備
情報セキュリティ設計	「政府機関の情報セキュリティ対策のための統一基準」(情報セキュリティ政策会議決定)、及び各府省の情報セキュリティポリシーに準拠して情報セキュリティ設計を行うこと	基本設計 詳細設計
テスト環境のセキュリティ対策	テスト環境（機器、作業室、テストデータ等）を受注者が用意する場合は、これらの環境に対しては充分なセキュリティ対策を実施すること	単体テスト･結合テスト･総合テスト
利用者教育	システム利用者向けに、情報セキュリティに関する教育を行うこと。	利用者教育
情報セキュリティ管理	各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと。また、発生した場合には発注への迅速な報告を行った上で被害を最小限に抑えること	プロジェクト管理

●6.4.運用

留意点	留意点の概要	TRM での記載箇所
運用体制の取り扱い	体制図等の個人情報の記載がある場合、当該文書は、規程に定める重要度に応じた取り扱いとする。	運用計画の策定

●6.5. ヘルプデスク

役務項目	役務の概要	TRM での記載箇所
情報セキュリティ対策実施要領作成	ヘルプデスク運用計画の中で、情報セキュリティ対策実施要領を作成し、府省と協議の上決定すること。	運用計画の策定
ヘルプデスク要員教育	ヘルプデスク要員に対して、ヘルプデスクを行う際に、実施すべき情報セキュリティ対策に関して教育を実施すること。	作業環境の整備

●6.6.1. ハードウェア保守

役務項目	役務の概要	TRM での記載箇所
ファームウェアの更新、設定変更等	ＢＩＯＳなどセキュリティやハードウェアの安定性に関係するファームウェアは常に最新の情報を入手し、必要に応じた更新作業の実施をハードウェア保守事業者に求めること。	バージョンアップの支援

●6.6.2. ソフトウェア保守

役務項目	役務の概要	TRM での記載箇所
セキュリティパッチの情報提供	ソフトウェアのバグ、パッチ及びバージョンアップ等に関する情報は入手次第、アプリケーション保守事業者又はシステム基盤保守事業者に通知し、パッチ適用前の事前適用をアプリケーション保守事業者、又はシステム基盤保守事業者に指示する必要がある。 早急なパッチ適用可否を判断するために、ソフトウェア保守事業者が提供するソフトウェアバージョンアップ等の情報提供先にアプリケーション保守事業者、システム基盤保守事業者を加える方法もある。	修正（パッチ）ファイル、バージョンアッププログラムの提供

●6.6.4. システム基盤保守

役務項目	役務の概要	TRM での記載箇所
セキュリティパッチの情報提供と適用	情報システムに関する技術的問題、セキュリティ脆弱性（セキュリティホール)、ソフトウェアのバグ、パッチ及びバージョンアップ等に関する情報を、速やかに府省庁に報告すること。 また、府省庁の要求に応じて、パッチの適用可能性検証作業、適用作業パッチ等の適用作業及びソフトウェアの技術相談への対応を行うこと。	システム基盤ソフトウェアのアップデート

●6.7. 機器調達付帯作業

留意点	留意点の概要	TRM での記載箇所
セキュリティ設計	「政府機関の情報セキュリティ対策のための統一基準」(情報セキュリティ政策会議決定)、及び各府省の情報セキュリティポリシーに準拠してセキュリティ設計書を作成し、それに準じた情報セキュリティ対策を実施すること	現地調査･設計
セキュリティの 設定･調整	現行システムに係わる手順書、導入方法や作成したセキュリティ設計書を用いてに本システムに必要な環境設定、各種調整作業を行うこと	機器のセットアップ
ウイルス定義ファイルの更新	ウイルスソフト･ウイルス定義ファイルが常に最新の状態にあるよう更新を行うこと	機器のセットアップ

●6.8. iDC 設備調達付帯作業

留意点	留意点の概要	TRM での記載箇所
セキュリティ監視	セキュリティ状況監視（ファイアーウォールのログの精査、不正侵入の監視等）ならびに監視結果の定期的に府省担当者への報告を行うこと	運用･保守（日次）
セキュリティ診断と報告	定期的に脆弱性の診断を行い、その結果（状況、影響、対応方法）を府省担当者に報告すること	運用･保守（月次）

●6.9. ネットワーク調達

留意点	留意点の概要	TRM での記載箇所
情報セキュリティの定義	情報資産の重要度とリスクに応じた情報セキュリティ対策を､「政府機関の情報セキュリティ対策のための統一基準」に基づく各府省の情報セキュリティポリシーに準拠して、具体的に定義する。	設計･開発計画
情報セキュリティ要件（対策）	セキュリティ対策として、市場に認知されている対策全般を行うために、省のセキュリティポリシー、セキュリティガイドラインに従うこと。 運用にあたっては、セキュリティレベルを維持すること。また、ネットワーク全体で講じなければならないセキュリティ対策については、現行運用保守業者と協力、調整して行うこと	設計･開発
機器の廃棄	不要機器を破壊する場合以外について、撤去対象機器の撤去･搬出後、第三者がデータ復元ソフトウェア等を利用してもデータが復元されないように完全にデータを消去すること。	設計･開発
セキュリティ設計	セキュリティポリシー設計(暗号化、FW、IDS/IPS、検疫)、暗号化設計（暗号化仕様、暗号化方式、暗号化アルゴリズム）等を実施するか、仕様と同様に提示された規定に従うこと。	設計･開発
セキュリティ検査	導入するネットワーク機器の脆弱性について、第三者機関等において検証･公開されることがあり、問題がある場合は対応をすること。	設計･開発
セキュリティテスト	情報セキュリティに関するテストの実施を確実に行うこと。 導入するネットワーク機器の脆弱性について、第三者機関等において検証･公開されることがあり、問題がある場合は対応をすること。	テストと移行判定支援
インシデント対応	ネットワークに関する障害情報及びセキュリティインシデントを迅速に受けられる連絡体制を確立すること。	運用･保守業務

セキュリティ診断と報告	回線のトラフィック状態を常時監視すること。異常なトラフィック等があった場合には、早急に原因調査を行い、現行運用保守業者を経由して担当職員に報告をすること。	運用･保守業務
セキュリティ検査	導入するネットワーク機器の脆弱性について、改善の必要性が指摘された場合には、迅速に対応すること。	運用･保守業務

6.12.6.セキュリティに特化した役務調達

（作成を予定）

6.13.その他

（作成予定）

7.推奨される技術標準

本章では、政府の情報システムの調達の際に優先的に調達されるべき技術標準の例と、それを選択する際の指針を示す。

推奨される技術標準の選定指針を策定するにあたっては、以下の 2 つの資料を参照した。

- 情報システムに係る相互運用性フレームワーク （平成 19 年 6 月）
  http://www.meti.go.jp/press/20070629014/siryou.pdf
- TRM 第 1 版:妥当性検証報告書 （平成 16 年 2 月）
  http://www.ipa.go.jp/software/optimize/pdf/technicalveri.pdf

また技術標準は調達指針が示す分離調達を実施する観点から選ばれたものであり、調達される技術すべてを網羅するものではない。

7.1.「情報システムに係る相互運用性フレームワーク」による技術標準要件

以下は「情報システムに係る相互運用性フレームワーク」に記載されている一文である。

> 政府公共機関の情報システム構築に係る選択肢の拡大と、公正で透明性のある調達及び適正な価格でより質の高い情報システムを調達するためには、情報システムの新規開発及び改修において、ベンダー独自技術への依存を廃し、政府情報システムにおけるさらにオープン化を推進する必要がある。
>
> 「情報システムに係る政府調達の基本指針」において、政府は、設計・開発の工程については原則として、共通基盤システム、個別機能システムの単位での分離調達を行う旨の方針を示している。この基本指針に従って分離調達された個別機能システムは、共通基盤を介して統合され、個別機能システムが共通基盤と、もしくは個別機能システム同士が互いに情報を交換することにより、それぞれの個別機能システムとして、さらに統合された全体システムとして業務に要求されるすべての機能が実現されなければならない。つまり、個別機能システム間及び個別機能システムと共通基盤の間での相互運用性が要求されることになる。

このように、情報システムの分離調達が今後の方針であるとともに、「分離調達」と「オープン化」を推進しながら、「相互運用性」を第一に考えた技術標準選定が必要となる。さらに、政府調達では、公平で公正な調達が大前提となることから、「オープンな標準」の選定を目指すことが最重要課題となる。

7.1.1.「オープン化」と「オープンな標準」の定義

「情報システムに係る相互運用性フレームワーク」では、「オープン化」を以下のように定義している。

> 情報システムを個別調達及び交換可能な標準部品に分解することによって、調達及び保守・運用におけるベンダー独自技術への依存を小さくし、調達及び保守・運用サービスに参入できる業者の数を増大させること。

ここで「オープンな標準」とは、原則として以下のすべてを満たしている技術標準をいう。

- 開かれた参画プロセスの下で合意され、具体的仕様が実装可能なレベルで公開されていること
- 誰もが採用可能であること
- 技術標準が実現された製品が市場に複数あること

7.1.2.標準技術としての妥当性を確保するための要件

「情報システムに係る相互運用性フレームワーク」では、TRM から参照される技術は、標準技術としての妥当性を確保するために、仕様の標準化の観点から以下が要求されている。

- 標準化機関等により標準仕様として標準化された技術であるか、又は標準化されつつある技術であること。
- 知的財産権（IPR: Intellectual Property Right）の扱いが標準化の際に明確にされており、不当な課金の可能性なしに誰もが自由にその仕様を実装できること。

そして、技術要件の観点から、以下を技術標準選択の検討事項としている。

- 情報システムの相互運用性を確保するため、標準仕様に準拠した実装同士の相互接続に成功した実績があるか、あるいはそのような実績が上がる見込みがあるか（相互接続性の検証）。
- 情報システムの可搬性を確保するため、標準仕様に準拠した実装上で、あるアプリケーションが同じ仕様に準拠した異なる実装上への移植に成功した実績があるか、あるいはそのような実績が上がる見込みがあるか（可搬性の検証）。
- 情報システムが将来にわたって活用され、継続的な拡張やメンテナンスが可能になるような機能や特徴、例えば拡張容易性や特定プラットフォームからの独立性等を備えていること。（将来への継続性の検証）。
- TRM は府省におけるフロントオフィス業務、ミドルオフィス業務及びバックオフィス業務を適用の対象としているため、これらの業務に必要で適用可能な技術であること（現行システムとの親和性の検証）。

7.1.3.技術標準に求められる指針

「情報システムに係る相互運用性フレームワーク」では、情報システムの設計者、調達担当者が遵守すべき指針が提示されている。原則的にはこの指針に従って技術標準も選定されることが望まれる。以下、その

指針を示す。

- 分離調達を行う際に、応札者を増やすためには、分離される機能単位が稼動する物理的なコンピュータや、プラットフォームに対しての制限を与えないことが望ましい。
- 技術部品間の相互運用性と技術部品単位での交換可能性を確保するため、上位レイヤーの技術部品は下位レイヤーの技術部品が提供する機能、インタフェースのうち、オープンな標準が必須と規定する機能及びインタフェースをのみ使用する標準部品で構成されている必要がある。
- 機能部品単位の分離調達及び選択肢の拡大を考えるのであれば、可能な限り機能部品が動作するプラットフォームを限定すべきではない。そのため、性能、セキュリティ、安定性等の非機能要件が許すのであれば、外部機能呼出しのためのサービス基盤としてプラットフォーム非依存のサービス基盤を選択することが望ましい。
- 長期間蓄積される、又は複数の利用者によって交換再利用されるデータのデータ形式としては、オープンな標準のデータ形式を採用することが望ましい。データ形式に関するオープンな標準が複数ある場合は、プラットフォームや特定技術への依存度の低い XML を用いたものを優先的に採用し、XML を用いたオープンな標準が複数存在する場合には、その形式をサポートする製品・ベンダーが複数存在するもののうち、市場性を考慮してより多くの製品・ベンダーに支持されると予想されるものを優先的に採用する。
- 機能部品単位の分離調達及び選択肢の拡大を考えるのであれば、可能な限り機能部品が動作するプラットフォームを限定すべきではない。そのため、機能部品間で交換されるメッセージの形式も、選択された外部機能呼出しのためのサービス基盤が許す範囲で、プラットフォーム非依存であることが望ましい。
- 機能部品間で交換されるメッセージの形式としては、プラットフォームへの依存性が低く、メッセージの論理構造をスキーマとして明示的に記述できる XML を使うことが推奨される。XML のスキーマはオープンな標準のスキーマを優先的に採用し、必要があれば拡張を施すものとする。また外部のシステムとの相互運用性が必要となる場合には、採用したスキーマを公開するものとする。
- 「政府調達に関する協定」第六条第二項に従い、調達仕様で参照する標準は、国際規格及び日本工業規格を優先する。対応する国際規格又は日本工業規格が存在しない場合は、次いでそれ以外のオープンな標準を参照する。

7.2.「TRM 第 1 版：妥当性検証報告書」における技術標準の評価項目

平成 16 年度に作成された TRM 第 1 版における重要技術を選定するに際しては、以下を評価項目とした。

- 評価対象の技術が、標準化団体により標準仕様として標準化された（あるいはされつつある）技術であることを、評価項目の 1 つとする。
- また、標準化された仕様が広く実装され、普及するためには、仕様に含まれる知的財産権の扱いが標準化の際に明確にされており、不当な課金の可能性なしに誰もが自由にその仕様を実装できることが重要である。そこで標準化については、この知的財産権の取扱い状況も考慮する。

- 情報システムの相互運用性（Interoperability）を確保するため、標準仕様に準拠した実装同士の相互接続に成功した実績があるか(あるいはそのような実績が上がる見込みがあるか)を、技術面での評価項目の 1 つとする。
- 情報システムの可搬性（Portability）を確保するため、標準仕様に準拠した実装上で、あるアプリケーションが同じ仕様に準拠した異なる実装上への移植に成功した実績があるか（あるいはそのような実績が上がる見込みがあるか）を、技術面での評価項目の 1 つとする。
- 情報システムが将来にわたって活用され、継続的な拡張やメンテナンスが可能になるような機能や特徴、例えば拡張容易性（Scalability）や特定プラットフォームからの独立性（Independence）、等を備えていることを、技術面での評価項目の 1 つとする。
- TRM は府省におけるフロントオフィス業務、ミドルオフィス業務及びバックオフィス業務を適用の対象としているため、これらの業務に必要で適用可能な技術であることを、技術面での評価項目の 1 つとする。
- 特定の技術を実際のシステムに導入し、継続的に活用するため、対象となる技術が実用性・将来性をもったものであることを評価項目の 1 つとする。

7.3.推奨される技術標準の選定指針

7.3.1.評価基準と評価項目

「情報システムに係る相互運用性フレームワーク」と「TRM 第 1 版：妥当性検証報告書」から導き出される推奨される技術標準選定に際して、オープン性、公平性、業務要件への適合性、相互運用性、潜在的発展性、政府規制の可能な限り独立した 6 つの評価基準にしたがって対象となる技術標準を評価すべきである。評価に際しては、定量的な評価を心がけるべきである。また、調達対象及び調達を行う組織（府省）独自の事情を勘案し、以下にあげる各評価基準の重みづけを適切に設定する必要がある。以下、各評価基準について説明する。

7.3.1.1.オープン性

これは一般に、特別な条件や障壁なく情報を入手したり、あるいは標準規格の取り巻く状況（審議状況など）を利害関係者が十分に把握できる状態を表す。結果として、技術的観点から、標準規格や制定団体が、特定のベンダーやグループにのみ利益がもたらされるような仕組みにならないよう配慮されていることなども含まれることになる。

このように、オープン性という評価基準は対象範囲が広いため、「標準制定団体・委員会参加のオープン性」、「メンテナンス・サポート体制を含む意思決定プロセスのオープン性」、「公開された技術仕様のオープン性」、「IPR ポリシーのオープン性」、「データ形式のオープン性」、「ベンダー独立性」、「プラットフォーム独立性」の7つに分類し、評価項目を策定した。具体的な評価項目を7つの分類毎に示す。

a) 標準制定団体・委員会参加のオープン性

標準仕様を制定している団体が特定の利益集団に依存しない標準化機関であること。かつ特定の団体の利益を目的とする標準化機関ではないこと。利害関係者を含め誰もが一定の条件を満たせば、標準化機関

や審議委員会に参加可能であること。かつ上記の一定の条件が、参加者の所属や、思想、意見の表明、利害関係を制限するものではないこと。

b) メンテナンス・サポート体制を含む意思決定プロセスのオープン性

標準仕様の内容への変更要求の受け付けなど、審議がオープンな形で実施できるように明確で理解しやすい意思決定プロセスを有すること。さらに、特定の利益集団に依存しない中立な組織が責任を持って標準仕様をメンテナンス／サポートする体制が整っていること。

c) 公開された技術仕様のオープン性

標準仕様が完全な形で一般に公開され、すべての人が同じ条件で標準仕様を入手できること。

d) IPR ポリシーのオープン性

IPR ポリシーに関する条件が明確に宣言されていること。

e) データ形式のオープン性

″交換可能性″という観点で、他アプリケーションとの交換が可能なデータ形式であること。″データ形式の独立性″の観点で、特定プラットフォーム、特定アプリケーションに依存しないデータ形式であること。″データの属性を記述できる標準の積極採用″という観点で、データ形式に関するオープンな標準が複数ある場合はデータの属性を記述できる標準/スキーマ形式の標準が存在する標準を優先的に採用すること。特に、″使用スキーマの公開″という観点では、外部のシステムとの相互運用性が必要となる場合には、採用したスキーマを公開すること。

f) ベンダー独立性

標準仕様が、特定ベンダーの製品や独自技術に依存していないこと。

g) プラットフォーム独立性

標準仕様に準拠した情報システムが将来にわたって活用され、継続的な拡張やメンテナンスが可能になるように、特定プラットフォームから独立していること。例えば、業界標準(XML スキーマ)の優先採用など、(XML のスキーマは)オープンな標準(のスキーマ)を優先的に採用すること。

7.3.1.2.公平性

これは、規格制定団体における様々なプロセスや規格自体の運用が公平におこなわれているかに関わる評価基準である。規格制定プロセスや規格の内容に、何らかの差別的条件や障壁が設けられていたり、特定の利害関係者を優位に立たせたり、逆に不利な立場に置かないことを目的としている。公平性はオープン性と混同されがちだが「標準規格評価基準」では明確に分けている。これに類する評価項目は以下の通りである。

a) 標準策定プロセスの公平性

初期の提案から最終的な標準承認に至るまでの複数の段階が設けられ、それぞれの段階において提出

されるドラフトのレベルや審議内容などの合意が得られていること。

b） コンセンサスを原則とする意思決定
審議プロセスにおいては、全員の合意を取るための努力がはらわれなければななららい。

c） 意思決定に関する公平性
審議プロセスに参加しているすべての人・組織は、意思決定に際し、それぞれが持つ権利を行使できること。

d） 設定されている IPR ポリシーの公平性
標準仕様の利用に影響を与える IPR ポリシーは、すべての利用者に公平かつ合理的であり、不当な課金の可能性無しに実装できること。（例：ロイヤリティ・フリー）

e） 公平なメンテナンス・サポート体制
標準仕様のメンテナンス／サポートにおいて、特定のベンダーやアプリケーションに有利になることがあってはならない。

7.3.1.3.業務要件への適合性

これは、標準規格が開発目的や機能要件、さらに利用者のニーズにどの程度応えているかを測るための評価項目である。具体的な評価項目は以下の通りである。

a） 標準仕様に対する妥当性
標準仕様は、特定の問題を解決するために有用かつ実用的なものでなければならない。

b） 標準制定団体に対する妥当性
標準仕様を制定する団体は、特定の問題を解決するために有用かつ実用的な仕様を制定しなければならない。

c） 機能要件への対応度
標準仕様は、特定の要件の解決するための技術を包含したものでなければならない。

d） 利用者・適用対象の明確度
誰がどのような問題を解決するためにその標準仕様を使えばよいかが明確になっていなければならない。

e） 標準利用指針策定
標準仕様の規定内容に選択の余地がある場合など、標準仕様の実際の利用における統一を図るための指針が定められなければならない。（例：プロファイル、ガイドライン）

7.3.1.4.相互運用性

これは、標準規格に準拠した複数の製品やサービス間でデータのやり取り、他製品との置き換え、バージョン間での互換性、他のシステムとの接続性などを可能とし、様々な側面で実装されるシステムがベンダーロックインされることを防ぐための評価基準である。これに関する具体的な評価項目は以下の通り。

a) 可搬性の担保

標準仕様に準拠した実装上のアプリケーションが同じ仕様に準拠した異なる実装上への移植に成功した実績があるか、あるいはそのような実績が上がる見込みがあること。

b) 標準/仕様間相互運用性

複数の標準仕様間の相互利用可能性を実現すべく、同等の機能を持つ複数の標準仕様が存在する場合には、利用者にとって最適な標準仕様を選択できるように、それらの間での互換性がなければならない。

c) バージョン間互換性

既存標準との親和性を確保すべく、既存システムにも適用可能な技術であること。そのために、関連標準との上位互換性が確保されていること。

d) システム間相互運用性

他システムとの親和性を図るべく、上位アプリケーションを含め、他のシステムとの連携が容易であること。

7.3.1.5.潜在的発展性

標準規格を選択することによる結果、選択によるインパクト、標準規格自体の将来的な発展性など、標準規格の間接的な効果を計るための評価基準である。これに分類される具体的な評価項目は以下の通り。

a) 拡張容易性

将来にわたって活用され継続的な拡張やメンテナンスが可能になるように、標準仕様が当初想定していた適用分野以外にでも容易に適用させることができる機能を備えたものであること。

b) スケーラビリティ

標準仕様の規定が、対象物のサイズや数が多くなっても対応可能なものであること。

c) 技術内容の将来性

（例えば先進的な技術であっても）将来に亘って発展が見込めるもの。

d) 標準仕様の普及度

その標準仕様に適合し、利用者が複数の中から選択できるに十分な数の独立した別個のベンダーによる実装製品が存在しなければならない。また、(XML のような)オープンな標準が複数存在する場合には、より多くの製品・ベンダーに支持されると予想されるものを優先的に採用すること。

e) 技術内容の成熟度

具体的仕様が実装可能なレベルで公開されていること。また、標準仕様が長期間に渡って使われることにより、発見された仕様の不備などが修正され、安定して使える状態になっていることが望ましい。

7.3.1.6.政府規制

日本政府が政策として産業界一般に課している要件が存在する。特に、政府調達では、その遵守が求められているため、それらも標準規格選定の際の評価項目の一つとなる。具体的な評価項目の例をあげる。

a) アクセシビリティ

政府のアクセシビリティ要件を満たすもの。

b) セキュリティ

政府のセキュリティ基準を満たすもの。

c) グリーンIT

環境目標の達成に貢献するもの。

d) プライバシー

政府の「個人情報の保護に関する基本方針」に従うもの。

7.3.2.標準の分類と評価基準

情報技術に関する標準の適用分野は多岐にわたっている。適用分野の異なる標準を全て同一の評価基準で一律に評価することは非効率である。そのため、情報技術に関する標準を下記に示すように 9 つに大きく分類し、この分類ごとの評価基準を、共通の評価基準とは別に設ける。なお、単一の標準であっても適用分野が広い標準は、複数の分類に属す場合があることに注意を払う必要がある。

7.3.2.1.メタデータ定義

データ定義を行うための記法等の構文、意味を定義する仕様。

7.3.2.2.データ定義

バイナリ形式のデータフォーマット、テキスト形式のデータ記述を定義するための仕様。定義されたデータフォーマットを作成するためのアルゴリズムの記述を含む場合もある。定義方法は、既存のメタデータ定義仕様を用いる場合もあるし、データ定義仕様の中で自らの定義仕様を定義する場合もある。後者の場合は、メタデータ定義の属性も持つことになる。

7.3.2.3. 定義

用語の定義、対応表、コード表など。データ形式そのものを定義する仕様。

7.3.2.4.アルゴリズム定義

アルゴリズムを実現するための記法の構文、意味を定義するための仕様。定義のための記法は、(BNF など)メタデータ定義が使われる場合がある。アルゴリズムで操作するデータの定義方法を含む場合がありうるが、その場合には、データ定義の属性を持つ。

7.3.2.5.プレゼンテーション

計算機内のデータをユーザに提示あるいは、ユーザの指示を計算機に伝えるために必要となる変換規則及びその使用方法のガイドラインを定めるための仕様。

7.3.2.6.API

他のプログラムに対して機能を提供するインタフェースを定義するための仕様。API の標準仕様は、プログラムの組み合わせの自由度を向上させることを目的とする。呼び出す側のプログラムから利用するために必要な以下のようなことを言語バインディングの形式で定義する。呼び出すための前提条件、呼び出すための名称、提供される機能、呼び出すときに受け渡す必要のある情報、正常に処理された場合や何らかの異常があった場合の動作。

7.3.2.7.プロトコル

複数のプログラムが協調してある機能を実現する場合に、複数のプログラム間のやりとりの以下のようなことを定義するための仕様。あるまとまった機能を実現するための呼び出しの順番、個々の呼び出しで実現される機能、個々で受け渡すデータ形式。しばしば、下位のプロトコル仕様の機能を前提として上位のプロトコル仕様が定められる場合がある。プロトコルをプログラムから利用する場合には、API の定義が必要となる。

7.3.2.8.アルゴリズム

処理方式そのものを規定する仕様。暗号化方式、データ圧縮方式などを規定する仕様。

7.3.2.9.プロセス

組織・個人等の活動プロセスを規定する仕様。また、プロセスが規定に従っているかどうかを監査する方法を規定する仕様。製品等が標準に準拠していることを試験するための方法の規定を含む。

7.4.推奨される技術標準

以下に政府の情報システムの調達の際に優先的に調達されるべき技術標準の例を示す。ちなみに、ここに掲載されている技術標準はあくまでも例であり、今後、推奨される技術標準の選定指針に従った調査結果によって内容の充実や改変が行われることがある。

【TRM_STD】 ISO/IEC 10646

推奨標準:

ISO/IEC 10646:2003 Information technology – Universal Multiple – Octet Coded Character Set (UCS)
ISO/IEC 10646:2003/Amd 1:2005 Glagolitic, Coptic, Georgian and other characters
ISO/IEC 10646:2003/Amd 2:2006 N'Ko, Phags-pa, Phoenician and other characters

JIS X0221:2007 国際符号化文字集合(UCS)

備考(特記すべき推奨理由等):

ISO/IEC 10646 は、世界各国の文字を集め、それに符号化を施した標準文字集合。ISO/IEC JTC1 で標準化され、現在ほとんどの OS、インターネット上のアプリケーションで標準対応しており相互運用性が実証されている。

【TRM_STD】 TCP/IP

推奨標準:

IETF FC 791: Internet Protocol

IETF RFC 793: Transmission Control Protocol

備考(特記すべき推奨理由等):

TCP/IP (Transmission Control Protocol/Internet Protocol)は、インターネットやイントラネットの標準プロトコル。OSI 参照モデルの第 3 層(ネットワーク層)を IP、第 4 層(トランスポート層) を TCP が担当する。インターネットの基本プロトコルとして Web を含むあらゆるインターネットシステムで実装されており、相互運用性が実証されている。また、現在のインターネットが存続する限り使われるプロトコルとして将来への継続性ももっている。

【TRM_STD】HTTP

推奨標準:

IETF RFC 2616 HyperText Transfer Protocol – HTTP/1.1

JIS TS X 0085:2004 ハイパーテキスト転送プロトコル HTTP/1.1

備考(特記すべき推奨理由等):

HTTP は、クライアント/サーバ間の要求・応答型のプロトコル。このプロトコルを使って XML 等のテキストデータが交換される。HTTP は、現在のすべての Web システムによって実装されている Web の基本プロトコルであり、相互運用性は実証されている。また、伝送されるデータのタイプを MIME タイプで指定することができ、柔軟性を備えると同時に拡張容易性をもつ。現在の Web が存続する限り使われるプロトコルとして将来への継続性もある。

【TRM_STD】SQL

推奨標準:

ISO/IEC 9075-1:2003

Information technology – Database languages – SQL – Part 1: Framework (SQL/Framework)

ISO/IEC 9075-2:2003

Information technology – Database languages – SQL – Part 2: Foundation (SQL/Foundation)

ISO/IEC 9075-3:2003
Information technology – Database languages – SQL – Part 3: Call-Level Interface (SQL/CLI)
ISO/IEC 9075-4:2003
Information technology – Database languages – SQL – Part 4: Persistent Stored Modules (SQL/PSM)
ISO/IEC 9075-9:2003
Information technology – Database languages – SQL – Part 9: Management of External Data (SQL/MED)
ISO/IEC 9075-10:2003
Information technology – Database languages – SQL – Part 10: Object Language Bindings (SQL/OLB)
ISO/IEC 9075-11:2003
Information technology – Database languages – SQL – Part 11: Information and Definition Schemas (SQL/Schemata)
ISO/IEC 9075-13:2003
Information technology – Database languages – SQL – Part 13: SQL Routines and Types Using the Java TM Programming Language (SQL/JRT)
ISO/IEC 9075-14:2006
Information technology – Database languages – SQL – Part 14: XML-Related Specifications (SQL/XML)

備考（特記すべき推奨理由等）：
SQL は、リレーショナル・データベース上でのデータの定義及び操作を行うための照会言語。ISO/IEC JTC1 の規格である SQL は、現在あらゆるリレーショナル・データベース製品で実装されている。リレーショナル・データベースの基礎言語として、リレーショナル・データベースが存続する限り使われる将来への継続性をもつ。

【TRM_STD】LDAP (Lightweight Directory Access Protocol)

推奨標準：
IETF RFC 4511　Lightweight Directory Access Protocol (LDAP): The Protocol

備考（特記すべき推奨理由等）：
LDAP は、ネットワークを利用するユーザ名やマシン名等の様々な情報を管理するディレクトリデータベースにアクセスするためのプロトコル。多くのベンダーの実装によって広く普及しており、相互運用性が実証されている。

【TRM_STD】XML（eXtensible Markup Language）

推奨標準：
W3C eXtensible Markup Language (XML) 1.0
JIS X 4159:2002 拡張可能なマーク付け言語 (XML) 1.0

備考（特記すべき推奨理由等）：
XML は、構造化されたデータをテキスト形式で表現するための汎用データ記述言語。テキストだけで記

述されるので、「6.1.3. 技術標準に求められる指針」にも説明があるように、プラットフォームや特定技術への依存度が低く独立性を保てる。また、メッセージの論理構造をスキーマとして明示的に定義できるため、あらゆる分野で利用することが可能であり、拡張容易性を備えると同時に相互運用性を備えている。文書コンテンツの表現やアプリケーションの内部構造の表現に至るまであらゆる分野で利用が進んでおり、将来への継続性ももつ。さらに、複数の異なるプラットフォーム上に XML を用いるミドルウェアやアプリケーションが開発され、それらの間で XML データのやり取りが行える実績もあるため、可搬性の要件も満たしている。

【TRM_STD】XML Schema

推奨標準:

W3C XML Schema Part 1: Structures Second Edition

W3C XML Schema Part 2: Datatypes Second Edition

備考(特記すべき推奨理由等):

W3C の XML Schema(Part1 及び Part2)は、個別のアプリケーションや仕様ごとに XML のタグセットを定義するためのスキーマ記述言語。スキーマは XML の要素,属性及び要素間の階層構造を定義するものであり、現在流通している XML 業界標準のほとんどすべてが W3C XML Schema を使用している。また、ツールやアプリケーションでもほとんどすべてが W3C XML Schema に対応しており、相互運用性が実証されている。XML データ構造を定義する言語として情報構造の再定義も容易であり、拡張容易性も備えている。

【TRM_STD】WSDL (Web Services Description Language)

推奨標準:

W3C Web Services Description Language (WSDL) 1.1

備考(特記すべき推奨理由等):

WSDL は、Web サービスの所在、Web サービス・アプリケーションと交換するメッセージ形式等、Web サービスの機能とそれを利用するためのインタフェースを記述する枠組みを規定した言語。WSDL を提供するサービスやそれを生成するツールが多数存在し、WS-I Basic Profile では、WSDL の相互運用性を保証するプロファイルを規定している。記述形式には XML が採用されているため、特定の OS からの独立性があり、容易に拡張可能でもある。また、SOA でも利用される等将来への継続性も見られる。

【TRM_STD】WS-I Basic Profile

推奨標準:

ISO/IEC PRF 29361

Information technology - Web Services Interoperability - WS-I Basic Profile Version 1.1

備考(特記すべき推奨理由等):

WS-I Basic Profile は、SOAP や WSDL 等の Web サービス関連規格の様々な機能の利用法に関する指

針を示すプロファイル。これによって製品間での Web サービスの相互運用が高まる。Web サービス関連規格の発展に伴い新たな規格をプロファイルに取り込む等、将来への継続性ももっている。

【TRM_STD】SOAP

推奨標準:

W3C Simple Object Access Protocol (SOAP) 1.1

備考(特記すべき推奨理由等):

SOAP は、Web サービスを呼び出すための基本プロトコル。SOAP によるメッセージのやり取りを行うための接続実験等も様々な業界で行われており、サポートしている製品も多数存在する。DOPG(旧:分散オブジェクト推進協議会)では、SOAP の製品間接続性が確認され、実用的なレベルでの相互運用性をもつことが実証されている。また、記述形式には XML が採用されており、特定の OS からの独立性があり、容易に拡張可能な仕様となっており、将来的にも継続した利用が見込まれる。

【TRM_STD】X.509

推奨標準:

ISO/IEC 9594-8:2001

Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

JIS X5731-8:2003 開放型システム間相互接続 - ディレクトリ - 第 8 部 認証の枠組み

備考(特記すべき推奨理由等):

X.509 は、公開鍵証明書の標準形式や証明書パス検証アルゴリズム等を規定したもの。X.509 による電子証明書は各国電子政府での電子認証にも使われ、政府系の認証局のほか、民間の認証局も数多く存在する。これらが連携して PKI を構成しており、相互運用性が実証されている。X.509 は ITU-T の国際規格としての改訂作業も漸進的に進められており、将来への継続性もある。

付録1　調達事例

１．政府共通

情報システムに係る政府調達事例データベース：
国の行政機関で調達された案件を対象
http://cyoutatujirei.e-gov.go.jp/

２．各府省庁局の調達仕様書（案）等

内閣府：
情報システムに係る政府調達について
 <公益認定等総合情報システム>、<経済財政政策関係業務等に必要なシステムに係わる業務・システム>など
http://www.cao.go.jp/others/kichou/it/gyouseijouhou.html

人事院：
人事院政府調達情報
＜一般競争入札公告＞、＜意見招請に関する公示＞など
http://www.jinji.go.jp/tyoutatu/index14.4.1.htm

金融庁：
調達に関する情報
http://www.fsa.go.jp/common/choutatu/index.html

警察庁：
情報システム政府調達情報
http://www.npa.go.jp/chotatu/seifu_choutatsu/seifu_choutatsu.html

総務省：
総務省内の調達情報提供、大臣官房会計課、政府調達情報/企画競争・公募等
http://www.soumu.go.jp/menu_sinsei/cyoutatsu/cyoutatsu.html

総務省統計局、政策統括官（統計基準担当）、統計研修所の調達情報、入札公告
http://www.stat.go.jp/info/chotatsu/mokuji.htm

政府統計共同利用システムの設計・開発
http://www.stat.go.jp/info/guide/public/05/kaihatsu.htm

外務省：

外務省調達情報

http://www.e-procurement.mofa.go.jp/kokuji/SyuruiSentaku.html

財務省：

（省全体）政府調達情報

http://www.mof.go.jp/jouhou/tyoutatu/seihutyoutatu.htm

東京税関の調達情報

http://www.customs.go.jp/kyotsu/chotatsu/tokyo.htm

厚生労働省：

情報システムの調達にかかる調達情報の公表

http://www.mhlw.go.jp/sinsei/chotatu/chotatu/index.html

農水省：

入札情報（情報システムに関する政府調達の情報）

http://www.maff.go.jp/j/supply/index.html

経済産業省：

（省全体）入札情報一覧

http://www.meti.go.jp/information_2/publicoffer/00_bid_news_list.html

その他：

経済産業省 CIO/CTO 研修、５．調達支援資料中の付録の提案依頼書テンプレート

http://www.meti.go.jp/policy/it_policy/CIO/index.html

経済産業省システム開発に係る外注仕様書作成マニュアル（案）平成１５年７月２８日意見募集

http://www.meti.go.jp/feedback/data/i30728aj.html

３．各府省庁局の調達計画書

人事院：人事・給与関係業務システムの設計・改修等に係る調達計画書

http://www.jinji.go.jp/tyoutatu/systemtyoutatujyoho.htm

内閣府：電子内閣府の推進、情報システムに係る政府調達について

http://www.cao.go.jp/others/kichou/it/gyouseijouhou.html

警察庁：情報システム政府調達情報、調達計画書
http://www.npa.go.jp/chotatu/seifu_choutatsu/keikakusyo/keikakusyo.html

金融庁：調達に関する情報
http://www.fsa.go.jp/common/choutatu/index.html

総務省：情報システム調達計画書
http://www.soumu.go.jp/menu_sinsei/cyoutatsu/joho_system.html

外務省：情報システムに係る政府調達の基本指針による調達計画書の公表
http://www.mofa.go.jp/mofaj/annai/shocho/chotatsu/keikakusho/index.html

財務省：情報システム調達計画書の公表
http://www.mof.go.jp/jouhou/tyoutatu/seihutyoutatu.htm

東京税関：システム系調達計画書
http://www.customs.go.jp/kyotsu/chotatsu/sonota/s_tokyo.html

文部科学省：情報システムに係る政府調達計画書
http://www-gpo3.mext.go.jp/kanpo/keikakuidx.htm

厚生労働省：調達計画書
http://www.mhlw.go.jp/sinsei/chotatu/chotatu/keikakusho.html

農林水産省：調達計画書
http://www.maff.go.jp/j/supply/nyusatu/system/index.html

経済産業省：システム系調達計画書
http://www.meti.go.jp/information/publicoffer/sysplan.html

特許庁：特許庁運営基盤システム調達計画書について
http://www.jpo.go.jp/cgi/link.cgi?url=/koubo/choutatu/keikakushyo/kiban_system.htm

国土交通省：情報システムに係る政府調達の基本方針に基づく公表
http://www.mlit.go.jp/chotatsu/chotatsushishin/chotatsushishin.html

気象庁：調達計画書
http://www.data.jma.go.jp/chouta/data/H20/H20jouhousystem/jouhousystem.html

４．総合評価基準事例

人事院：人事・給与関係業務情報システムの機器・ソフトウェア賃貸借及び保守、評価手順書
http://www.jinji.go.jp/tyoutatu/090727_nyusatu.htm

内閣府：景気統計システム、調達仕様書その他提案依頼書に添付する関係文書（2008.10)、その３
http://www.cao.go.jp/kanbou/gyouseijouhou.html

付録2　役務調達仕様書例

第６章　役務調達の各節で参考とした仕様書例を記す。
なお、「TRM実証」は参考文献の情報処理振興機構　「技術参照モデルの実証的評価」調査報告書　2009年7月中の調達仕様書一式を表わす。

1.　全体計画策定支援

2.　調達支援

①　要件定義

府省庁	調達仕様書名	作成年度
経済産業省	平成22年度 次期経済産業省基盤情報システム要求仕様書作成等支援業務	H22

②　プロジェクト管理

府省庁	調達仕様書名	作成年度
厚生労働省	労災レセプト電算処理システムの構築に係る工程管理等支援業務	H21
法務省	登記・供託オンライン申請システムの統合プロジェクト管理支援業務調達　調達仕様書	H21
人事院	人事・給与関係業務情報システムの設計・改修等に係るプロジェクト管理支援業務　一式	H21
総務省	総合無線局監理システムにおける設計・開発・運用等業務に係るプロジェクト・マネジメント支援等業務の請負	H22
農水省	平成22年度森林保険業務システム構築事業支援業務仕様書	H22

3.　システム構築（設計・開発）

①　新規開発

府省庁	調達仕様書名	作成年度
TRM実証	①行政情報提供_調達仕様書（TRM有版）	H20
TRM実証	②グループウェア等職員情報システム調達仕様書（TRM有版）	H20
TRM実証	④-1運用管理システム調達仕様書（TRM有版）	H20
厚生労働省	医科レセプトのオンライン請求における代行請求用ソフトウェアの開発業務一式に係る入札仕様書	H21
厚生労働省	労災レセプト電算処理システムに係る設計・開発等業務一式調達仕様書（案）	H21
厚生労働省	日本年金機構間接業務システム開発等業務一式要求仕様書	H21
内閣府	公益認定等総合情報システム	H19

② システム更改

府省庁	調達仕様書名	作成年度
外務省	在外経理システムの業務・システム最適化計画」に伴う開発作業　一式 仕様書	H20
厚生労働省	汎用申請・届出等省内処理システム更改	H20
財務省	国庫事務電算化システム開発業務 一式 調達仕様書（案）	H21
法務省	登記情報提供システムの更新に係る 調達仕様書案	H21
法務省	出入国管理業務の業務・システム最適化に係る次世代外国人出入国情報システムの設計・開発・テスト等及び統合データ管理システムの改修に関する仕様	H22
環境省	平成22年度から平成23年度までの環境省電子申請・届出システムの再構築に係る設計等業務調達仕様書（案）	H21
気象庁	土砂災害警戒情報作成システムの製作・借用（リース）及び保守並びに取付調整	H22
総務省	次期小売物価統計調査システム設計開発等業務の請負 提案依頼書	H22
総務省	統計調査等業務に係る各府省共同利用型システムの設計・開発等業務の請負 提案依頼書	H18
農水省	生鮮食料品流通情報データ通信システムの設計･開発 調達仕様書	H20
厚生労働省	医科レセプトのオンライン請求における代行請求用ソフトウェアの開発業務一式に係る入札仕様書	H21
厚生労働省	労災レセプト電算処理システムに係る設計・開発等業務一式調達仕様書（案）	H21
厚生労働省	日本年金機構間接業務システム開発等業務一式要求仕様書	H21
TRM実証	①行政情報提供_調達仕様書（TRM有版）	H20

③ ハードウェア更改

府省庁	調達仕様書名	作成年度
外務省	外務省 情報公開事務支援システム 仕様書	H20
外務省	旅券申請書画像ファイリング・システム一式 調達仕様書	H20
法務省	地図情報システムの機器更新に伴うデータ移行及びシステム切替等作　調達仕様書	H22
国土交通省	自動車保有関係手続のワンストップサービスシステム 業務アプリケーション移植業務	H20
内閣府	公益認定等総合情報システム	H19
厚生労働省	医科レセプトのオンライン請求における代行請求用ソフトウェアの開発業務一式に係る入札仕様書	H21
厚生労働省	労災レセプト電算処理システムに係る設計・開発等業務一式調達仕様書（案）	H21
TRM実証	①行政情報提供_調達仕様書（TRM有版）	H20

④　機能追加

府省庁	調達仕様書名	作成年度
外務省	地域別・国別ODA供与目標額システムの改修」に係る業務一式　仕様書	H20
外務省	条約等国際約束検索システムのアプリケーション開発及びデータ移行に関わる調達　仕様書	H20
経済産業省	STATS移行に係る新世代統計システムメンテナンス（データ検証機能追加）	H21
経済産業省	経済産業省調査統計システムへの移行に係るツール等機能作成及びデータベース移行等　一式	H21
厚生労働省	職業安定行政関係システム（仮称）雇用保険業務処理機能群及び助成金機能群開発業務	H20
財務省	法人企業統計調査等ネットワークシステムの標本抽出の見直し対応等改修業務提案依頼書	H22
財務省	通関情報総合判定業務機能（CIS　機能）のプログラム改変仕様書	H20
財務省	他業務・システム最適化実施に伴う財政融資資金電算機処理システム設計・開発業務　一式仕様書	H19
法務省	次期登記情報システムのアプリケーション機能追加開発の調達に係る仕様書	H20
法務省	法務省総合的な受付・通知システムの性能強化に係る役務調達仕様書	H20
法務省	地図情報システムにおける新オンライン申請システムとの連携に係る対応作業　調達仕様書	H21
海上保安庁	海上保安における船舶動静情報活用業務システム	H20
国土交通省	航空交通管制情報処理システム　管制支援処理システム一式の製造及び調整	H22
国土交通省	自動車登録識別情報システム　設計・開発	H21
人事院	人事・給与関係業務情報システムの業務機能強化のための設計・改修等業務	H21
人事院	人事・給与関係業務情報システムの集中化及び府省要望等への対応並びに制度改正への対応のための設計・改修　一式　仕様書	H20
人事院	人事・給与関係業務情報システムの届出申請機能等の設計・改修　一式	H21
人事院	人事・給与関係業務情報システム設計・改修	H20
総務省	暗号アルゴリズム移行に係る政府認証基盤の　検証環境の機能拡充のための設計・開発・構築等の請負	H21
総務省	総合無線局監理システムデータベース管理機能　設計・開発等の請負	H22
総務省	総合無線局監理システム基幹系機能拡充　設計・開発等の請負	H22
総務省	総合無線局監理システム情報系業務に関わる機能開発等の請負	H22
内閣府	総合防災情報システム換装・機能拡張・保守・運用業務	H21
農水省	森林保険業務システム構築事業改修及び本稼働準備業務仕様書	H21

4.　運用

府省庁	調達仕様書名	作成年度
TRM実証	⑤運用調達仕様書（TRM有版）	H20
外務省	外務省IT広報業務におけるCMS（コンテンツ・マネジメント・システム）運用・保守業務一式　調達仕様書	H21
外務省	官房業務システムの運用業務　一式	H21
経済産業省	経済産業省基盤情報システムにおけるサーバ・ネットワーク運用管理	H20
経済産業省	統計情報システム運用管理支援業務	H20
厚生労働省	監督・安全衛生等業務及び労災保険給付業務の業務・システム最適化に係る運用等業務一式	H20
厚生労働省	職業安定行政関係システム〈仮称〉統合運用監視業務（平成23年度運用開始）	H21
財務省	予算編成支援システムの維持管理	H21
法務省	債権譲渡登記次期システムに係る運用・保守及び登記所支援業務に関する調達仕様書	H20
金融庁	有価証券報告書等の開示書類に関する電子開示システム　EDINETシステム運用業務調達提案依頼書	H20
人事院	人事・給与関係業務情報システムに係るヘルプデスク支援業務　調達仕様書	H21
総務省	共同利用システム基盤の業務・システム最適化に係る運用請負（共同利用システム基盤における機器・ソフトウェア増設に伴う追加運用請負）	H21
総務省	電子政府利用支援センターの運用等の請負	H19
農水省	総合食料局情報管理システム運用支援業務	H19

5.　ヘルプデスク

府省庁	調達仕様書名	作成年度
厚生労働省	監督・安全衛生等業務及び労災保険給付業務の業務・システム最適化に係る運用等業務一式	H20
厚生労働省	職業安定行政関係システム〈仮称〉統合運用監視業務（平成23年度運用開始）	H21
財務省	予算編成支援システムの維持管理	H21
人事院	人事・給与関係業務情報システムに係るヘルプデスク支援業務　調達仕様書	H21
TRM実証	⑤運用調達仕様書（TRM有版）	H20

6.　保守

①　ハードウェア保守

府省庁	調達仕様書名	作成年度
外務省	文書作成編集システム一式（ハードウエア）の賃貸借及び保守業務の調達　仕様書	H20
厚生労働省	「監督・安全衛生等業務及び労災保険給付業務の業務・システム最適化に係る 拠点LAN導入及び保守業務一式」	H20
気象庁	火山監視・情報センターシステムのハードウェアの借用（リース）・保守及び取付調整	H21
農水省	国家森林資源データベースサーバ等保守業務仕様書　h220226_siyou_2	H21
TRM実証	④-1運用管理システム調達仕様書（TRM有版）	H20
TRM実証	④-2HW調達仕様書（TRM有版）	H20

②　ソフトウェア保守

府省庁	調達仕様書名	作成年度
人事院	人事・給与関係業務情報システムに係る機器・ソフトウェア賃貸借及び保守（第二期）	H21
TRM実証	④-1運用管理システム調達仕様書（TRM有版）	H20

③　アプリケーション保守

府省庁	調達仕様書名	作成年度
経済産業省	工業統計システムメンテナンス（運用環境整備）　一式	H21
厚生労働省	汎用申請・届出等省内処理システム更改　一式	H20
財務省	財政融資資金電算機処理システムの補正及び維持管理に係る請負契約 一式	H19
法務省	平成22年度新登記情報システムの業務アプリケーション保守業務の調達　調達仕様書	H21
気象庁	土砂災害警戒情報作成システムの製作・借用（リース）及び保守並びに取付調整	H22
金融庁	EDINET（有価証券報告書等の開示書類に関する電子開示システム）の運用改善に係る追加設計・開発等の調達仕様書（案）	H20
農水省	畑作物統計調査集計プログラムの修正業務　調達仕様書	H21
厚生労働省	次期労働保険適用徴収システムに係るアプリケーション保守業務 一式 仕様書	H21
人事院	人事・給与関係業務情報システムに係る機器・ソフトウェア賃貸借及び保守（第二期）	H21
TRM実証	①行政情報提供_調達仕様書（TRM有版）	H20

④　システム基盤保守

府省庁	調達仕様書名	作成年度
厚生労働省	平成21 年度以降に拡張する厚生労働省統合ネットワーク回線・機器に係る供給(設計・開発、結合・統合テスト等及び運用)調達仕様書	H21
厚生労働省	「監督・安全衛生等業務及び労災保険給付業務の業務・システム最適化に係る 拠点LAN導入及び保守業務一式・運用等業務」調達仕様書	H20
TRM実証	③　ネットワーク調達仕様書（TRM有版）	H20

7. 機器調達付帯作業

府省庁	調達仕様書名	作成年度
TRM実証	④-2HW調達仕様書(TRM有版)	H20
外務省	在留届電子届出システム用サーバ等　一式 調達仕様書	H20
外務省	電子入札・開札システム用機器一式の賃貸借・保守　調達仕様書	H21
経済産業省	経済産業省調査統計システム二次リリース用機器　一式	H22
経済産業省	経済産業省汎用電子申請システム用機器	H20
厚生労働省	職業安定行政関係システム(仮称)窓口受付機能群サーバ及び端末設備(平成21 年度導入分)等一式調達仕様書	H20
厚生労働省	職業安定行政関係システム(仮称)職業紹介サブシステムサーバ等一式調達仕様書	H21
財務省	財政融資資金電算機処理システムに係るハードウェア等機器 調達仕様書	H21
総務省	共同利用システム基盤の業務・システム最適化に係る機器・ソフトウェアの借入	H20
総務省	職員等利用者認証業務の業務・システム最適化に係る機器等の借入調達仕様書	H20
法務省	次期登記情報システム用端末装置等の調達に係る仕様書	H20
法務省	平成22年度新登記情報システム用端末装置等の調達　調達仕様書	H21

8. iDC設備調達付帯作業

府省庁	調達仕様書名	作成年度
TRM実証	⑦IDC_調達仕様書(TRM有版)	H20
外務省	データセンタ借入等一式	H22
厚生労働省	職業安定行政関係システム(仮称)データセンタ等一式	H20
法務省	新登記情報システム附帯設備の調達	H21
総務省	共同利用システム基盤の業務・システム最適化に係る施設・設備賃貸借の調達	H20

9. ネットワーク調達

府省庁	調達仕様書名	作成年度
TRM実証	③ネットワーク調達仕様書(TRM有版)	H20
TRM実証	⑥WAN_調達仕様書(TRM有版)	H20
外務省	外務省情報ネットワーク(共通システム)におけるオープンLAN基本業務システム構築及び運用一式調達仕様書	H20
経済産業省	経済産業省ネットワークサービス	H20
厚生労働省	厚生労働省ネットワークシステムの更改に係る調達	H21
厚生労働省	平成21 年度以降に拡張する厚生労働省統合ネットワーク回線・機器に係る供給(設計・開発、結合・統合テスト等及び運用)調達仕様書	H21
法務省	平成２ ２ 年度新登記情報システム通信サービスの調達	H21

付録3　別表　暗号アルゴリズムの移行指針について

政府機関の情報システムにおいて広く使用されている暗号アルゴリズム SHA-1 及び RSA1024 については、現在、安全性の低下が指摘されているところであり、これらをより安全な暗号アルゴリズムへ移行させることが求められている。

その際には、情報システムの相互運用性を確保するなどの観点から、政府統一的な対応をとる必要があるため、情報セキュリティ政策会議第１７回会合（平成２０年４月２２日）において「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（別添）を決定した。

現在、政府機関で使われている暗号アルゴリズム SHA-1 及び RSA1024 について、当該移行指針に従って「２０１４年度早期の対応完了」に向けた情報システムの整備、更新を進めているところである。また、急激な安全性の低下に備え、あらかじめ緊急避難的な対応（コンティンジェンシープラン）を検討しているところである。

なお、各府省庁における当該移行指針に従った暗号移行及びコンティンジェンシープランの策定については、政府機関全体としての情報セキュリティ水準の向上を図るための対策基準を定めた「政府機関の情報セキュリティ対策のための統一基準」（情報セキュリティ政策会議決定）においても明記されている。

また、暗号アルゴリズムの移行に関しては、急激な状況変化も想定されるため、最新の状況を収集し、対応することが望まれる。

1 現状と課題

①電子政府システムでは，電子署名等のために暗号が使用されており，SHA-1及びRSA1024と呼ばれる暗号方式を広く使用．
②しかし，このSHA-1及びRSA1024は，安全性の低下が指摘されており，より安全な暗号方式への移行が必要．
③より安全な暗号方式への移行にあたっては，情報システムの相互運用性確保や政府全体の情報セキュリティの向上のため，政府統一的な移行指針を策定することが必要．

2 暗号の移行指針の概要

①技術的な対応

【政府認証基盤とそれに依存する各府省庁の情報システム】

○ 相互運用性確保のため，新旧暗号方式の双方に対応し，適切な時期に暗号方式を切り替える運用を可能に．

○ 新たな暗号方式として，SHA-256及びRSA2048を採用．

○ 移行完了前に安全性低下の影響が発生する場合に備え，緊急避難的な対応も想定．

【上記以外の情報システム】

○ 現実的な脅威となる攻撃手法が示された時点で，速やかに別の暗号方式に変更する等の対応措置を可能とする．

○ 新たな暗号方式は，より安全なものを各府省庁において判断し決定する．

②制度的な対応

○ 各府省庁において次を実施
・システムの移行時期を踏まえ，必要な対応の取りまとめ
・移行手順書の整備

③スケジュール

○ 内閣官房，総務省，法務省，経済産業省等
新たな暗号方式へ切り替える時期等を2008年度中に検討．

○ 内閣官房，総務省等
相互接続の技術要件，緊急避難対応等について2008年度中に検討．

○ 各府省庁
2010年から2013年までの間に，各情報システムの対応を完了．

○ 内閣官房，総務省，経済産業省
安全性の状況を監視し，必要な情報を速やかに各府省庁に提供．

図 付録 3-1 暗号の移行指針の概要

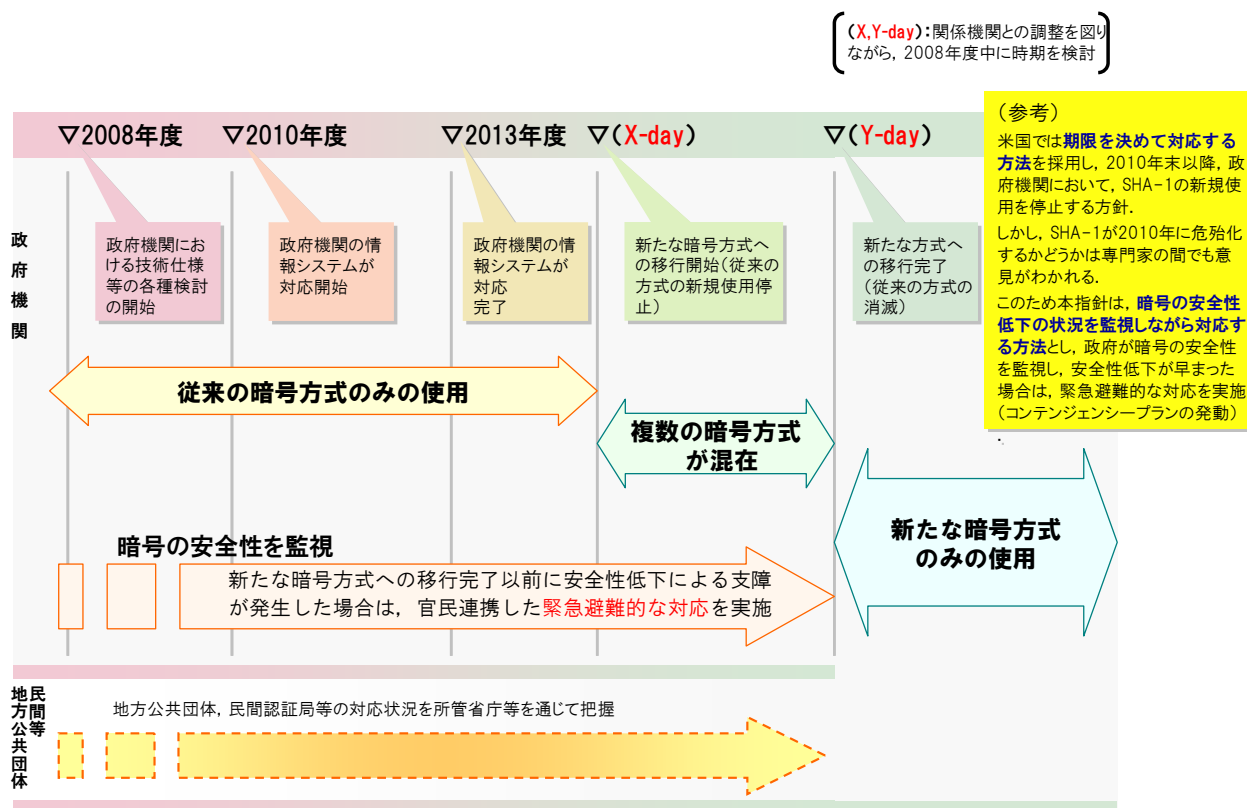



図 付録 3-2 移行指針に基づく暗号方式の移行完了までのスケジュール

付録4　参考文献

■業務・システム最適化指針　2006 年 3 月
電子政府の総合窓口　電子政府の推進について
http://www.e-gov.go.jp/doc/scheme.html

■情報システムに係る政府調達の基本指針　2007 年 3 月
総務省ホームページ
http://www.soumu.go.jp/s-news/2007/070301_5.html

■「情報システムに係る政府調達の基本指針　実務手引書」（第二版）
総務省ホームページ
http://www.soumu.go.jp/menu_news/s-news/2007/070919_2.html

■情報システムに係る相互運用性フレームワーク　2007 年 6 月
経済産業省ホームページ
http://www.meti.go.jp/press/20070629014/20070629014.html

■経済産業省ナレッジポータル参照モデル（TRM）　2005 年 3 月
経済産業省ホームページ　ＥＡポータル
http://www.meti.go.jp/policy/it_policy/ea/data/report/index10.html

■「ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針」2007 年　11 月
総務省ホームページ
http://www.soumu.go.jp/menu_news/s-news/2007/071127_3.html

■データセンターの安全・信頼性に係る情報開示指針（第 1 版）　2009 年 2 月
総務省ホームページ
http://www.soumu.go.jp/main_content/000010165.pdf

■「ASP/SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」2009 年 7 月
総務省ホームページ
http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000010.html

■「Service Organization Control Reports (formerly SAS 70 reports)」
http://www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/SOC/Pages/SORHome.aspx

■「日本公認会計士協会の監査基準委員会報告書第 18 号「委託業務に係る統制リスクの評価」(通称：18 号監査)」

■内閣官房情報セキュリティセンター　主要公表資料
「政府機関の情報セキュリティ対策のための統一基準(第 4 版)(平成 21 年度修正)」
http://www.nisc.go.jp/active/general/pdf/K303-091.pdf

「政府機関の情報セキュリティ対策のための統一基準(第 4 版)(平成 21 年度修正)」解説書
http://www.nisc.go.jp/active/general/pdf/K303-091C.pdf

注:2011 年 4 月 21 日に政府機関統一基準の最新版が公開された。
・政府機関の情報セキュリティ対策のための統一規範(2011 年 4 月 21 日)
http://www.nisc.go.jp/active/general/pdf/kihan.pdf

・政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針 (2011 年 4 月 21 日)
http://www.nisc.go.jp/active/general/pdf/unyou.pdf

・政府機関の情報セキュリティ対策のための統一管理基準 (2011 年 4 月 21 日)
http://www.nisc.go.jp/active/general/pdf/K304-101.pdf

・政府機関の情報セキュリティ対策のための統一技術基準 (2011 年 4 月 21 日)
http://www.nisc.go.jp/active/general/pdf/K305-101.pdf

・「政府機関の情報セキュリティ対策のための統一管理基準」解説書
http://www.nisc.go.jp/active/general/pdf/K304-101C.pdf

・「政府機関の情報セキュリティ対策のための統一技術基準」解説書
http://www.nisc.go.jp/active/general/pdf/K305-101C.pdf

・リスク要件リファレンスモデル作業部会報告書 (2010年3月)
http://www.nisc.go.jp/inquiry/pdf/2-1_RM-model_Open.pdf

・情報システムに係る政府機関におけるセキュリティ要件策定マニュアル (2011 年 3 月 30 日)
http://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf

■オンライン手続におけるリスク評価及び電子署名・認証ガイドライン
各府省情報化統括責任者（CIO）連絡会議第４１回（2010 年 8 月）決定
http://www.kantei.go.jp/jp/singi/it2/cio/dai41/41gijisidai.html

■電子政府ユーザビリティガイドライン
各府省情報化統括責任者（CIO）連絡会議第37回（2009年7月）決定
http://www.kantei.go.jp/jp/singi/it2/cio/dai37/37gijisidai.html

■情報処理振興機構　「技術参照モデルの実証的評価」調査報告書　2009 年 7 月
情報処理振興機構ホームページオープンソフトウェア利用促進事業成果一覧（2008 年度）
http://www.ipa.go.jp/software/open/ossc/2008seika.html
・調査報告書：
http://www.ipa.go.jp/software/open/ossc/download/trm20_report.pdf
・エグゼクティブサマリー:
http://www.ipa.go.jp/software/open/ossc/download/trm20_report_summary.pdf
・エグゼクティブサマリー補足資料:
http://www.ipa.go.jp/software/open/ossc/download/trm20_report_summary_appended.pdf
・調達仕様書一式:
http://www.ipa.go.jp/software/open/ossc/download/trm20_specific_procurement.zip
・総合評価基準書(機能)一式:
http://www.ipa.go.jp/software/open/ossc/download/trm20_assessment_1.zip

・総合評価基準書(全般)一式:
http://www.ipa.go.jp/software/open/ossc/download/trm20_assessment_2.zip
・提案依頼書一式:
http://www.ipa.go.jp/software/open/ossc/download/trm20_rfp.zip

■情報処理振興機構　SEC BOOKS「共通フレーム 2007 第 2 版」 2009 年 10 月
http://sec.ipa.go.jp/press/20090930_b.html